

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

ZAJIŠTĚNÍ KVALITY SLUŽEB V DATOVÝCH SÍTÍCH

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

PETR MAREČEK

BRNO 2015



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



**FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH
TECHNOLOGIÍ**
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

ZAJIŠTĚNÍ KVALITY SLUŽEB V DATOVÝCH SÍTÍCH

QUALITY OF SERVICE ENSURENCE IN DATA-NETWORKS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

PETR MAREČEK

VEDOUCÍ PRÁCE
SUPERVISOR

doc. Ing. JAROSLAV KOTON, Ph.D.

BRNO 2015



VYSOKÉ UČENÍ
TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: Petr Mareček

ID: 154801

Ročník: 3

Akademický rok: 2014/2015

NÁZEV TÉMATU:

Zajištění kvality služeb v datových sítích

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte problematiku zajištění kvality služeb v paketově orientovaných sítích. Navrhněte jednoduchou podobu DiffServ domény, kdy na využitích aktivních prvcích sítě ukážete a popíšete procesy v nich probíhající. Navrženou síť prakticky realizujte použitím aktivních prvků Mikrotik, kdy popíšete jejich nutnou konfiguraci. Koncové stanice připojené do sítě využijte jako zdroj a cíl datových toků náležících do oddělených tříd, kdy tak ukážete charakteristické vlastnosti nastavení sítě.

DOPORUČENÁ LITERATURA:

[1] MEDHI, D., RAMASAMY, K.: Network Routing: Algorithms, Protocols, and Architectures, Morgan Kaufmann, ISBN: 978-0-12-088588-6, 2007.

[2] CHAO, H.J., LIU, B.: High Performance Switches and Routers, Wiley-IEEE Press, ISBN: 978-0-4700-5367-6, 2007.

Termín zadání: 9.2.2015

Termín odevzdání: 2.6.2015

Vedoucí práce: doc. Ing. Jaroslav Koton, Ph.D.

Konzultanti bakalářské práce:

doc. Ing. Jiří Mišurec, CSc.

Předseda oborové rady

UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

ABSTRAKT

Tato práce se zabývá problematikou zajištění kvality služeb v datových sítích. První část práce obsahuje teoretický rozbor, kde je popsána technologie Quality of Services a její mechanismy. V závěru teoretické části jsou rozebrány jednotlivé systémy front. Druhá část práce je zaměřena na návrh a realizaci laboratorní úlohy s cílem na prokázání teoretických znalostí a vyhodnocení vhodného systému front v závislosti na poskytnutých službách.

KLÍČOVÁ SLOVA

QoS, DiffServ, DSCP, DiffServ doména, fronta, směrovač

ABSTRACT

The thesis deals with the issue of ensuring the Quality of Service (QoS) in data networks. The first part is theoretical, where is described QoS technology and her mechanisms. At the end of the theoretical part, possible queuing systems are shortly presented. The second part of the thesis deals with the design and implementation of a laboratory exercise with the aim of proving theoretical knowledge and evaluating the suitability of a certain queuing system according to the provided services.

KEYWORDS

QoS, DiffServ, DSCP, DiffServ domain, queue, router

MAREČEK, Petr *Zajištění kvality služeb v datových sítích*: bakalářská práce. BRNO: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2015. 77 s. Vedoucí práce byl doc. Ing. Jaroslav Koton, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Zajištění kvality služeb v datových sítích“ jsem vypracoval(a) samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor(ka) uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil(a) autorská práva třetích osob, zejména jsem nezasáhl(a) nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom(a) následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

BRNO

.....

podpis autora(-ky)

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu doc. Ing. Jaroslavu Kotonovi, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

BRNO

.....

podpis autora(-ky)

PODĚKOVÁNÍ

Výzkum popsáný v této bakalářské práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

BRNO

.....
podpis autora(-ky)

OBSAH

Úvod	11
1 Služby provozu	12
1.1 Parametry QoS	12
1.2 Hlasová služba (VoIP)	13
1.3 Obrazové služby	15
1.4 Datové služby	16
1.5 Řídící služby	17
1.6 Služby méně důležitého provozu	17
2 Mechanismy QoS	18
2.1 Mechanismus Integrovaných služeb (IntServ)	18
2.1.1 Značkování paketů	18
2.1.2 Protokol pro rezervaci prostředků (RSVP)	20
2.2 Mechanismus Diferencovaných služeb (DiffServ)	22
2.2.1 Značkování paketů	23
2.2.2 Klasifikace paketů	27
3 DiffServ doména	28
3.1 Hraniční směrovač	29
3.2 Páteří směrovač	30
4 Systémy front	31
4.1 Systém fronty typu FIFO	31
4.2 Prioritní systém front (Priority Queuing – PQ)	32
4.3 Systém front se spravedlivou obsluhou (Fair Queuing – FQ)	33
4.4 Systém front s váženou cyklickou obsluhou (Weighed Round Robin – WRR)	35
4.5 Systém front s váženou spravedlivou obsluhou (Weighted Fair Queuing – WFQ)	36
4.6 Systém založený na třídách s váženou spravedlivou obsluhou (Class-Based Weighted Fair Queuing – CB WFQ)	38
4.7 Systém založený na třídách s prioritní frontou (Low Latency Queuing – LLQ)	39
5 Návrh laboratorní úlohy	40
5.1 Návrh topologie	40
5.2 Nastavení koncových stanic a služeb	40

5.3	Konfigurace směrovače R1 a R2	42
5.3.1	Nastavení adresace a směrování	42
5.3.2	Model DiffServ domény	43
5.3.3	Nastavení procesů na směrovačích ve funkci hraničního a pá- teřního směrovače	46
5.3.4	Nastavení front	51
5.4	Ověření konfigurace a zhodnocení výsledků	56
6	Závěr	61
	Literatura	62
	Seznam symbolů, veličin a zkratk	64
	Seznam příloh	66
A	Návod k laboratorní úloze	67
A.1	Teoretický úvod	67
A.2	Pokyny k vypracování	71
A.2.1	Topologie a importování konfigurace	71
A.2.2	Doplnění konfigurace	72
A.2.3	Ověření nastavené konfigurace	75
B	Obsah přiloženého CD	77

SEZNAM OBRÁZKŮ

2.1	Struktura pole ToS podle [6].	19
2.2	Komunikace pomocí protokolu RSVP. [1]	21
2.3	Řízení provozu mechanismu IntServ. [1]	22
2.4	Struktura pole DS podle [13].	23
3.1	Model DiffServ domény. [2]	28
3.2	Postup zpracování paketů v hraničním směrovači. [2]	29
3.3	Postup zpracování paketů v páteřním směrovači. [2]	30
4.1	Princip systému fronty typu FIFO. [2]	32
4.2	Princip prioritního systému front. [2]	33
4.3	Princip systému front se spravedlivou obsluhou. [2]	34
4.4	Princip systému front s váženou cyklickou obsluhou. [2]	35
4.5	Princip systému front s teoretickým modelem bitové cyklické obsluhy. [2]	37
4.6	Ukázka příkladu datového provozu v systému WFQ. [2]	38
4.7	Princip systému založený na třídách s váženou spravedlivou obsluhou. [2]	39
5.1	Topologie laboratorní úlohy.	40
5.2	Grafické prostředí systému RouterOS v6.27 prostřednictvím aplikace <i>winbox</i>	42
5.3	Směrovací tabulky směrovače <i>R1</i> a <i>R2</i>	43
5.4	Zjednodušený model DiffServ domény.	44
5.5	Možné komunikace mezi stanicemi (a), znázornění komunikace mezi <i>VoIP serverem</i> a stanicemi (b).	46
5.6	Nastavení procesů hraničního a páteřního směrovače na směrovači <i>R1</i> a <i>R2</i>	47
5.7	Nastavení klasifikace a značkování paketů pro službu přenosu dat.	48
5.8	Nastavení klasifikace paketů pro službu přenosu dat.	50
5.9	Nastavení jednotlivých systémů front.	52
5.10	Nastavení fronty typu fifo.	53
5.11	Počet označkových, klasifikovaných a zařazených paketů pro prio- ritní systém front.	57
5.12	Rozdělení šířky pásma, konfigurací příslušných systémů front, mezi služby.	58
5.13	Počet označkových, klasifikovaných a zařazených paketů pro systém front s váženou cyklickou obsluhou.	59
A.1	Topologie laboratorní úlohy.	71

SEZNAM TABULEK

2.1	Základní rozdělení tříd podle hodnoty pole DSCP. [14]	24
2.2	Rozdělení tříd podle hodnoty pole DSCP v závislosti na PHB. [18]	26
A.1	Rozdělení tříd podle hodnoty pole DSCP v závislosti na PHB.	70

ÚVOD

V rámci současných datových a komunikačních sítí je provozováno mnoho služeb, které mají odlišné požadavky na parametry datového toku. Mezi tyto parametry patří zpoždění, proměnlivost zpoždění, ztrátovost a šířka pásma. S růstem poskytovaných služeb, a tedy i s růstem datového přenosu, dochází ke zpoždění, proměnlivosti zpoždění, ztrátě datových jednotek a k neefektivnímu využití šířky pásma. To vše má dopad na průběh služeb a na spokojenost zákazníka. Aby na straně zákazníka nedocházelo k nekvalitnímu poskytování služeb, byla vytvořena technologie zvaná Quality of Service, která je známá také pod zkratkou QoS. V základu je tato technologie podporována hlavně na aktivních síťových prvcích, které podporují síťovou vrstvu modelu TCP/IP. Poskytované služby a jejich požadavky na parametry QoS v datových sítích jsou popsány v 1. kapitole.

Implementace QoS je poskytnuta pomocí mechanismů IntServ a DiffServ. Tyto mechanismy používají rozdílné metody pro zajištění kvality služeb. Jejich důkladným popisem se zabývá 2. kapitola.

Ve 3. kapitole je popsána realizace mechanismu DiffServ, která je tvořena hraničními a páteřními směrovači. Tato realizace se označuje pojmem DiffServ doména. Protože je hlavním úkolem směrovače zajistit co nejrychlejší předání paketů k cílovému uzlu, je důležité, aby procesor nebyl vytížen jinými procesy. Proto se určité procesy, pro zajištění kvality služeb pomocí DiffServ, provádí jen na určitých místech v sítích.

S mechanismem DiffServ přichází proces značkování a klasifikace paketů. Proces značkování rozdělí jednotlivé pakety do tříd. Při zatížení síťových prvků dochází k řazení paketů do front. Do jaké fronty bude paket zařazen, rozhodne proces klasifikace. S pakety v daných frontách se pak zachází s různou prioritou podle třídy, do které paket patří. Řazení paketů do front a jejich systém odesílání na základě dané priority je popsán ve 4. kapitole.

V poslední 5. kapitole je popsána realizace vhodné laboratorní úlohy pro zajištění kvality služeb v datových sítích pomocí směrovačů od společnosti MikroTik. Laboratorní úlohu tvoří dvě koncové stanice, VoIP server a DiffServ doména. V laboratorní úloze je kladen důraz na ověření teoretických poznatků, konkrétně mechanismu DiffServ a jednotlivých systémů front. Výsledkem úlohy je zhodnocení použití vhodného systému front v závislosti na poskytovaných službách.

1 SLUŽBY PROVOZU

Pro efektivní zajištění kvality služeb je nezbytná znalost datového provozu. Přestože v současných datových sítích je provozováno velké množství různých služeb, je možné je rozdělit do dvou základních skupin. Základní dělení služeb se provádí podle jejich závislosti na čase. Pro některé služby je důležité, aby byly přeneseny s minimálním zpožděním, kdy určitá míra ztrátovosti je tolerována. Jedná se především o služby pracující v reálném čase. Mezi takové služby patří například přenos hlasu nebo videa. Druhou skupinou jsou pak služby, kde jejich přenos není závislý na čase. Tedy služby, u kterých není kvalita citlivá na zpoždění, ale klade velký důraz na nulovou ztrátovost. Jedná se například o přenos dat. Proces značkování paketů, který je popsán v kapitole 2.2.1, dále dělí jednotlivé služby do tříd. Podle rozdělení do tříd je každé službě přiřazena priorita, která určuje charakter zacházení s danou službou. Pro každou službu je třeba definovat parametry QoS (Quality of Services), které jsou klíčové k tomu, aby nedocházelo k degradaci dané služby. [1]

1.1 Parametry QoS

Kvalita služeb je závislá na několika parametrech. Mezi základní parametry patří ztrátovost paketů, zpoždění, kolísání zpoždění a šířka pásma. Citlivost na tyto parametry je pro každou službu jiná. [2]

Ztrátovost

Může nastat v případě zahlcení aktivních síťových prvků. Pokud je používán spolehlivý transportní protokol TCP (Transmission Control Protocol), jsou ztracené pakety posílány znovu. Nedochází tedy ke ztrátovosti paketů, ale ke zpoždění. Protokol TCP vyhovuje pouze službám nepracujícím v reálném čase. Pro služby pracující v reálném čase se používá nespolehlivý transportní protokol UDP (User Datagram Protocol), který ztracené pakety znovu neposílá. Protokol UDP klade důraz hlavně na rychlost přenosu.

Zpoždění

Zpoždění je doba, po kterou paket cestuje od zdroje k cílovému uzlu. Skládá se ze zpoždění způsobeného kódováním, paketizací, přenosem, zpožděním ve frontách a zpožděním při přepínání v síti. Pojem paketizace označuje dobu přípravy paketů pro přenos médii. Zpoždění ve frontě je závislé na typu fronty a služby. Služby pracující v reálném čase jsou náchylnější na zpoždění oproti službám nepracujícím v reálném čase. Pokud jsou tedy do fronty, která není typu FIFO, načteny služby

obojího typu, je zpravidla upřednostněna služba pracující v reálném čase. Zpravidla znamená, že upřednostněna může být i služba nezávislá na čase. Záleží pouze na správci sítě a jeho konfiguraci daného systému front. Jednotlivé systémy front jsou uvedeny v kapitole 4.

Kolísání zpoždění

Pakety nemusí v rámci daného přenosu přicházet všechny se stejným zpožděním neboli ve stejných intervalech. Kolísání zpoždění má největší význam pro hlasové služby a musí se řešit speciálními vyrovnávacími paměťmi. Kolísání zpoždění vzniká zejména v místech sítě, kde se spolu mísí různé toky do jediného výstupu.

Šířka pásma

Šířka pásma udává počet bitů, které je možné přenést za jednu sekundu. Pokud tedy je šířka pásma 64 kb/s, pak je možné přenést 64 000 b, neboli 8 000 B za sekundu. Šířka pásma je důležitá hlavně při poskytování služeb pracujících v reálném čase. Její hodnota je hlavně závislá na použitém přenosovém mediu podél celé trasy.

1.2 Hlasová služba (VoIP)

Jedná se o službu přenášející řečový signál. V dnešní době je pro přenos hlasové služby nejpoužívanější technologie VoIP (Voice over Internet Protocol). Kvalitní provozování hlasové služby pomocí VoIP klade v současnosti největší nároky na datové síť. VoIP se skládá ze dvou typů datového toku, konkrétně z přenosu samotného řečového signálu a z přenosu signalizačních informací. Požadavky na přenos těchto toků jsou odlišné. [3]

Požadavky na přenos řečového signálu

Kvalitní přenos řečového signálu klade velice přísné požadavky na datovou síť. Proto je tento typ provozu zpravidla zpracováván prioritně před jinými službami. Hlasová služba klade důraz na rychlý přenos, proto používá transportní protokol UDP. Na aplikační vrstvě modelu TCP/IP (Transmission Control Protocol/Internet Protocol) je používán protokol RTP (Real-Time Transport Protocol). V rámci DiffServ mechanismu je doporučeno zařazení hlasové služby do třídy EF. Třídy mechanismu DiffServ jsou blíže popsány v kapitole 2.2.1. Zajištění kvality hlasových služeb je závislé na parametrech QoS.

Prvním parametrem QoS je ztrátovost, která může způsobit degradaci hlasové služby. Ve výsledku může dojít ke ztrátě hovoru. Proto se ztrátovost eliminuje maskováním chybějícího úseku. Zvolený způsob maskování závisí na použitém kodeku a jeho implementované vlastnosti pro maskování ztrát. Kvalitu hlasové služby v závislosti na ztrátovosti paketů můžeme vyjádřit v procentech. Při ztrátě paketů do 2 % nedochází k poruše hovoru. Mezi 2 až 5 % pomalu dochází k nesrozumitelnosti hovoru. Pro 5 až 10 % je srozumitelnost nízká a znehodnocuje se kvalita hlasu. Pokud ztrátovost překročí 10 %, kvalita hovoru bude velice nízká, slyšitelnost minimální a nepomohou ani kvalitní kodeky proti odolnosti vůči ztrátám. [4]

Dalším parametrem, na který je hlasová služba velice citlivá, je zpoždění. Požadavky na zpoždění jsou přísnější než u ztrátovosti. Jestliže celkové zpoždění nepřesáhne hodnotu 150 ms, je tento hovor velmi kvalitní. Při zpoždění pod 20 ms nedochází k ozvěně v hovoru. Pro zpoždění mezi 150 až 400 ms považujeme hovor za přijatelný. Pokud hodnota přesáhne 400 ms, slyšitelnost mezi uživateli je špatná a může mezi nimi dojít i ke ztrátě synchronizace. [4]

Konstantní zpoždění v datových sítích, které fungují na principu přepínání paketů, není možné zajistit. Skutečné zpoždění přicházejících paketů kolísá kolem určité střední hodnoty. Přijaté pakety musí být zpracovány v pravidelných intervalech, proto se používá vyrovnávací paměť, tzv. jitter buffer. Aby nedocházelo k velké odchylce od střední hodnoty, přidává se v cílové stanici umělé zpoždění. Pokud je odchylka od střední hodnoty příliš velká, bude paket považován za ztracený. Je důležité si uvědomit, že toto umělé zpoždění bude součástí celkového zpoždění paketu. Pro kvalitní přenos řečového signálu by neměla hodnota kolísání zpoždění přesáhnout 30 ms. [2]

Šířka pásma je závislá na použitém kodeku a velikosti režijních informací. Mezi režijní informace patří velikosti hlaviček jednotlivých protokolů. Například pokud je velikost hlavičky pro IP (Internet Protocol) protokol 20 B, pro UDP protokol 8 B a pro RTP protokol 12 B, pak velikost režijních informací je rovna 40 B. Nepočítá se s velikostí režijních informací na nižších vrstvách modelu TCP/IP, tj. na vrstvě síťového rozhraní. Dále můžeme z paketizačního intervalu spočítat počet vygenerovaných paketů za sekundu, například 50 paketů při paketizačním intervalu 20 ms. Pak přenosová rychlost pro režijní informace bude $50 \cdot 40 \cdot 8 = 16 \text{ kb/s}$. Velikost dat při použití kodeku G.729, který používá frekvenci 8 kHz, a paketizačního intervalu 20 ms bude 160 B v každém paketu. Potom při rychlosti 50 paketů za sekundu dostaneme přenosovou rychlost $50 \cdot 160 \cdot 8 = 64 \text{ kb/s}$. Z rychlosti přenosu režijních informací a dat vidíme, že je potřeba vymežit šířku pásma 80 kb/s. Příklad byl převzat z [2].

Požadavky na přenos signalizačních informací

Požadavky na přenos signalizačních informací jsou vysoké, protože přenos těchto informací společně s řečovým signálem zajišťuje efektivní provozování hlasové služby. Konkrétně se jedná o signalizační protokoly, které určují charakter služby. Nejčastěji se signalizační protokoly zařazují do třídy CS3, konkrétně do třídy AF31. Více informací o daných třídách je uvedeno v kapitole 2.2.1. Pokud jsou však překročeny stanovené požadavky, může dojít k zařazení do tříd s větší pravděpodobností zahození paketů, konkrétně do třídy AF32 nebo AF33. Signalizační informace tvoří asi 2 až 5 % z celkové velikosti provozu služby. [2]

1.3 Obrazové služby

Z hlediska přenosu videa rozlišujeme dvě služby. Konkrétně se jedná o službu interaktivního videa a službu streamovaného videa. V případě interaktivního videa se jedná například o videokonferenci. Velmi známou aplikací, která poskytuje službu interaktivního videa, je například aplikace *Skype*. Služba streamovaného videa je využívána při jakémkoliv sledování videa v síti Internet. Požadavky na přenos těchto služeb jsou odlišné.

Požadavky na přenos interaktivního videa

Při videokonferenci se s přenosem obrazu přenáší také řečový signál. Platí zde tedy stejné požadavky jako pro přenos hlasové služby pomocí VoIP. Ztrátovost paketů by měla být maximálně do 2 %, zpoždění maximálně 150 ms a hodnota kolísání pod 30 ms. Doporučené zařazení je do třídy AF41, případně do tříd AF42 a AF43.

Videokonferenční přenos používá proměnlivou délku paketů a přenosovou rychlost. Délka paketů se běžně pohybuje kolem 129 až 256 B a 1025 až 1500 B. Samotný přenos video signálu nevyžaduje velkou rychlost přenosu. Pro přenos videokonferenční služby se často udává rychlost 384 kb/s. Musíme však počítat s přenosem řečového signálu a dalších režijních informací, které tvoří hlavičky jednotlivých protokolů. Proto se běžně pro videokonference rezervuje šířka pásma 460 kb/s. [2]

Požadavky na přenos streamovaného videa

Služba streamovaného videa neklade tak velké požadavky na přenos. Ztrátovost paketu může být až 5 % a zpoždění 4 až 5 s. Příchozí pakety se na straně cílového uzlu ukládají do paměti, která dokáže eliminovat i větší kolísání zpoždění. Doporučené zařazení této služby je do třídy CS4. Do jaké třídy bude tento provoz zařazen, je

však čistě na správci sítě. Pokud je potřeba tuto službu znehodnotit vůči jiným, je možné ji zařadit i do tříd nižších, např. do třídy CS1. [2]

1.4 Datové služby

Datové služby představují největší část síťového provozu. Zahrnují mnoho typů služeb, které mají odlišné požadavky na přenos. Proto byly definovány čtyři skupiny, které by měly vyhovět všem datovým aplikacím. [2]

Služby typu Best-Effort

Služby typu Best-Effort spadají do třídy, pro kterou je hodnota pole DSCP rovna hodnotě 0. Jedná se o třídu, která je znevýhodněna oproti všem ostatním třídám. Významem pole DSCP se zabývá kapitola 2.2.1. Mezi služby Best-Effort patří stovky až tisíce aplikací, proto je potřeba počítat s velkým datovým provozem. Je tedy důležité vymezit velkou šířku pásma pro tuto třídu. Většinou se doporučuje vymezení 25 % šířky pásma.

Služby s přenosem objemných dat

Hlavním požadavkem těchto služeb je nulová ztrátovost paketů. Na zpoždění a kolísání zpoždění nejsou kladeny žádné požadavky. Je výhodné tyto služby zařadit do samostatné třídy s přiřazenou určitou částí šířky pásma. Mezi základní představitele patří služba, která používá protokol FTP (File Transfer Protocol). Tento typ provozu se řadí do třídy CS1, konkrétně do třídy AF11. Pokud jsou však překročeny stanovené požadavky, může dojít k zařazení do tříd s větší pravděpodobností zahození paketů, konkrétně do třídy AF12 nebo AF13.

Transakční a interaktivní služby

Pojmem transakční služby se rozumí služby typu klient/server, např. komunikace se vzdáleným serverem pomocí protokolu Telnet. Jedním z hlavních požadavků je kromě ztrátovosti také zpoždění. Jedná se o komunikaci, která probíhá v daný okamžik mezi klientem a serverem. Proto je důležité, aby odezva serveru byla co nejrychlejší. Mezi interaktivní služby patří služby komunikačního typu, např. *ICQ*. Požadavky jsou podobné jako u transakčních služeb. Tento typ služeb je často řazen do třídy AF21. V případě překročení stanovených požadavků dojde k zařazení do třídy AF22 nebo AF23.

Uživatelsky kritické služby

Jedná se o služby, jejichž data jsou velmi důležitá. Konkrétní definování těchto služeb je pouze na správci sítě. Zpravidla to jsou transakční a interaktivní služby, které jsou více upřednostněny. Mohou tedy být zařazeny do třídy AF31. Při překročení stanovených požadavků pak do třídy AF32 nebo AF33.

1.5 Řídící služby

V síti se kromě dat pro uživatele přenáší také data, která jsou určena pro správu a řízení sítí. Jedná se o směrovací protokoly a management sítě.

Směrovací protokoly

Směrovací protokoly jsou důležité pro chod celé sítě. Pomocí jejich zpráv se směrovače informují o topologii sítí, které jsou připojené na jejich rozhraní. Směrovače tak umí příchozí pakety předat dál k cílovému uzlu. Proto je nezbytné, aby směrovací protokoly byly ve směrovačích zpracovány přednostně. Jsou řazeny do samostatné třídy CS6 a CS7.

Management sítě

Management sítě zajišťují protokoly, které slouží pro konfiguraci směrovačů a pro získávání statistických informací o zpracovávaném provozu. Základním příkladem takového protokolu je SNMP (Simple Network Management Protocol). Protokoly pro management sítě jsou řazeny do třídy CS2.

1.6 Služby méně důležitého provozu

Služby méně důležitého provozu patří do třídy, která je znevýhodněna oproti běžnému provozu Best-Effort. Mezi služby méně důležitého provozu se řadí takové služby, které nejsou přínosem v síti a mají spíše zábavní charakter. Konkrétně jsou to služby typu peer-to-peer, síťové hry nebo sledování televize přes datovou síť. Pro třídu zahrnující tyto služby je vyhrazena jen malá část šířky pásma, takže při vytížení sítě se na tyto služby nedostane a síťové prostředky tak budou využity jen pro důležité a požadující služby.

2 MECHANISMY QOS

Starší síťové technologie provozované v sítích, které jsou založeny na přepínání paketů, poskytují všem službám stejný způsob zacházení. Pokud nějaký aktivní síťový prvek obdrží řadu různých služeb v rámci datového toku, pak jsou bez jakýchkoliv garancí předány na výstup. Každá služba je zpracována nezávisle na jiné. Z tohoto důvodu není možné zvýhodnit nebo znevýhodnit některé služby. Jestliže nastane zahlcení datové linky, pak může dojít k vyčerpání veškerých síťových prostředků. Například na směrovači může dojít k zaplnění fronty, pro jedinou službu bude využita celá šířka pásma a řada dalších síťových prostředků bude vyčerpána. Pro každou službu to bude mít jiný dopad. Pro službu nepracující v reálném čase je akceptováno zpoždění, ale nemůže dojít ke ztrátě paketů. Naopak pro službu pracující v reálném čase může dojít k určité ztrátě paketů, ale je zde velká citlivost na zpoždění. Z těchto důvodů byly popsány dva mechanismy, které používají rozdílné přístupy k zajištění kvality služeb. [2]

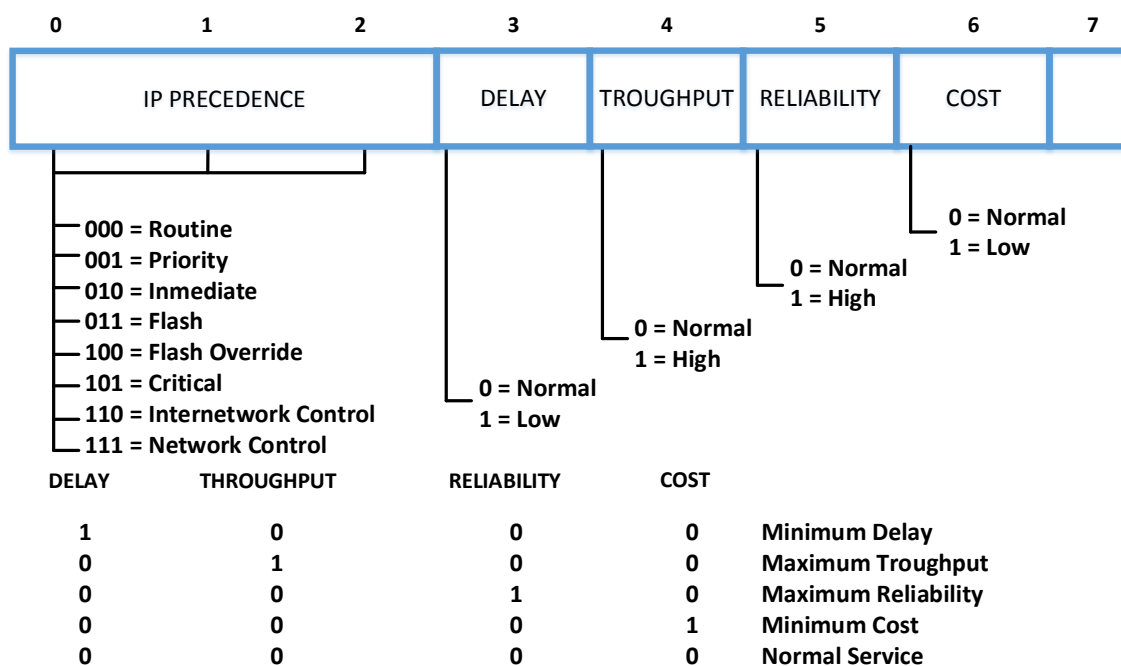
2.1 Mechanismus Integrovaných služeb (IntServ)

Mechanismus Integrovaných služeb je založen na rezervaci pásma a požadovaného zpoždění. Rezervace je vytvořena po celé komunikační trase, tzn. od zdroje k cíli. Mechanismus musí podporovat veškeré uzly sítě neboli směrovače, přes které spojení prochází. IntServ (Integrated Services) se skládá ze čtyř hlavních částí: plánovače paketů, kontroly přístupu, klasifikátoru a protokolu pro rezervaci prostředků RSVP (viz kap. 2.1.2). Plánovač paketů řídí zasílání jednotlivých toků dat. Je implementován v místech, kde jsou pakety řazeny do front. Většinou je každý tok dat řazen do samostatné fronty. Jak zacházet s pakety v jednotlivých frontách je hlavním úkolem plánovače. Další část se nazývá kontrola přístupu. Jedná se o rozhodovací algoritmus směrovače nebo hostitelské stanice. Pomocí algoritmu se rozhoduje, zda nová rezervace neovlivní již existující rezervaci. Identifikaci příchozích paketů a jejich následné rozdělení do tříd má za úkol klasifikátor. V dnešní době se jedná o zastaralou technologii. Před zahájením spojení vyžaduje velkou režii. Při použití v rozsáhlých sítích by tak docházelo k velké zátěži síťových prvků. Proto je její implementace vhodná například pro interní podnikové sítě. Podrobnější popis IntServ je obsažen v dokumentu RFC 1633 [5].

2.1.1 Značkování paketů

Proces značkování přiřadí jednotlivým paketům určitou prioritu, podle které je s pakety zacházeno. Jako příklad značky může být IP adresa zdroje nebo cílového uzlu.

Jednou z možností, která se používá pro značkování paketů, je nastavení pole Type of Services. Jedná se o pole v IP hlavičce, které se v protokolu IPv4 (Internet Protocol version 4) značí zkratkou ToS (Type of Services). Skládá se z osmi bitů. První tři bity určují prioritu specifikovanou typem služby. Další čtyři bity určují požadavky na přenos. Poslední bit je rezervován pro další použití. Směrovač tak musí při hledání cesty brát ohled i na požadavky definované nastavením pole ToS. Na obr. 2.1 je znázorněn význam jednotlivých bitů. [2]



Obr. 2.1: Struktura pole ToS podle [6].

IP precedence určuje prioritu, která byla danému paketu přiřazena na základě typu služby. Jelikož se tato část skládá ze tří bitů, je definováno osm prioritních úrovní. Doporučené přiřazení služeb k dané prioritní úrovni je následující:

- routine (0): zacházení s pakety je na úrovni Best-Effort,
- priority (1): pakety, které nevyžadují vysokou prioritu zpracování,
- immediate (2): správa sítě,
- flash (3): signalizační informace hlasových služeb,
- flash override (4): přenos videa,
- critical (5): hlasové služby,
- internetwork control (6): správa aktivních síťových prvků,
- network control (7): správa aktivních síťových prvků na úrovni lokální sítě.

Přiřazení služby k dané prioritní úrovni záleží na konfiguraci síťových prvků,

kterou provádí správce sítě. Po části IP Precedence následují čtyři bity, které signalizují způsob zpracování paketů. Čtvrtý bit pole ToS, který je označen slovem delay, indikuje požadavek na zpoždění. Pokud je jeho hodnota nastavena na logickou nulu, pak se jedná o normální zpoždění. V případě logické jedničky bude vyžadováno malé zpoždění. Označení throughput nese pátý bit, který indikuje propustnost. Stav logické nuly označuje normální propustnost. Vysoká propustnost je vyžadována, pokud je pátý bit pole ToS nastaven na logickou jedničku. Šestý bit, označen slovem reliability, klade požadavek na spolehlivost dané trasy. Stav logické nuly a jedničky mají podobný význam jako u pátého bitu. Logická nula označuje normální spolehlivost a logická jednička pak vysokou spolehlivost. Předposlední bit svým stavem určuje, jestli bude paket na směrovačích zvýhodněn před ostatními pakety. Využití tohoto bitu bylo poprvé uvedeno v dokumentu RFC 1349 [7]. Slovo cost v překladu znamená cena. Stav logické jedničky znamená nízkou cenu, proto bude paket zvýhodněn. Ve stavu logické nuly bude mít paket normální cenu a ke zvýhodnění nedojde. [6]

Po vysvětlení všech vlastností pole ToS si můžeme ukázat příklad pro značkování paketů pomocí tohoto pole. Logické stavy všech bitů budou nastaveny následovně: 10111000. Pak víme, že paketu je přidělena pátá priorita, tzn. critical. Z dalších čtyř bitů vidíme, že zpoždění bude nízké, propustnost vysoká, spolehlivost normální a cena také normální. Při takovémto nastavení pole ToS se může například jednat o hlasovou službu.

Pole ToS však nebylo běžně užíváno. Až později bylo toto pole využíváno mechanismem DiffServ, kterým se zabývá kapitola 2.2. Více informací o významu pole ToS je uvedeno v dokumentech RFC 1349 [7] a RFC 2474 [8].

2.1.2 Protokol pro rezervaci prostředků (RSVP)

Protokol RSVP (Resource Reservation Protocol) byl standardizován v RFC 2205 [9]. Jedná se o protokol, který zajišťuje předávání informací mezi sousedními uzly a rezervaci pásma pro konkrétní proces. V každém uzlu se snaží o vytvoření rezervace zdrojů pro daný tok dat. Hlavním úkolem je, aby v datových sítích mohly být podporovány odlišné výkonové požadavky pro různé služby. Při směrování využívá směrovací tabulky, ale nejedná se o směrovací protokol. RSVP pouze nastavuje kvalitu pro jednotlivé služby v uzlech sítě dané cesty. Koncové stanice komunikují pomocí zpráv PATH, RESV a dalších speciálních zpráv. Na obr. 2.2 je znázorněna komunikace pomocí protokolu RSVP. [10]

PATH

Pokud chce zdrojová stanice vytvořit novou rezervaci pro danou službu, vyšle zprávu PATH. Nese informaci o potřebné rezervaci a prochází všemi uzly sítě na cestě k cíli. Každý směrovač má uložen PATH stav. V tomto stavu je uložena IP adresa předchozího směrovače, která je potřebná pro zprávu RESV. [1]

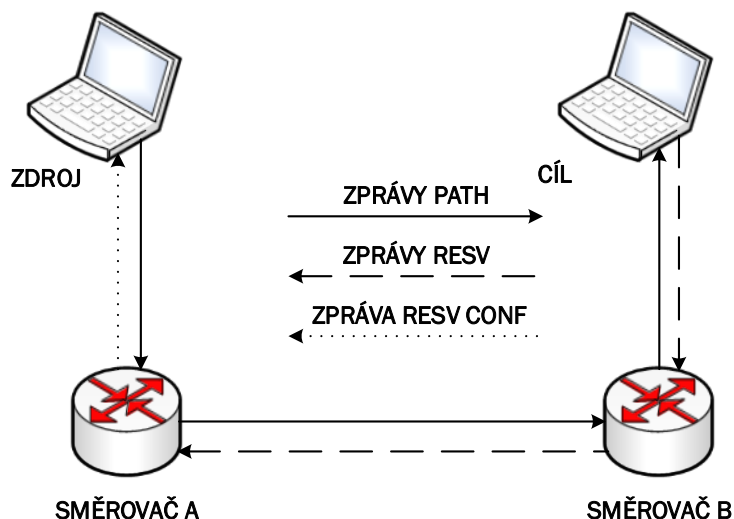
RESV

Jedná se o odpověď na zprávu PATH. Prochází stejnými uzly sítě, jakými přišla zpráva PATH. Pokud cílová stanice rezervaci zamítne nebo není možné danou rezervaci poskytnout v uzlech sítě, je poslána zpráva RESV ERR. Rezervace je vytvořena, pokud zdrojová stanice přijme zprávu RESV.

Speciální zprávy

Protokol RSVP poskytuje také jiné speciální zprávy pro komunikaci mezi zdrojovou a cílovou stanicí. Konkrétně se jedná o zprávy:

- PATH ERR: generuje se při chybném zasílání zprávy PATH,
- PATH TEAR: odstraní PATH stav ze všech směrovačů,
- RESV TEAR: odstraní rezervační stav ze všech směrovačů,
- RESV CONF: tuto zprávu obdrží zdrojová stanice pro finální potvrzení rezervace.

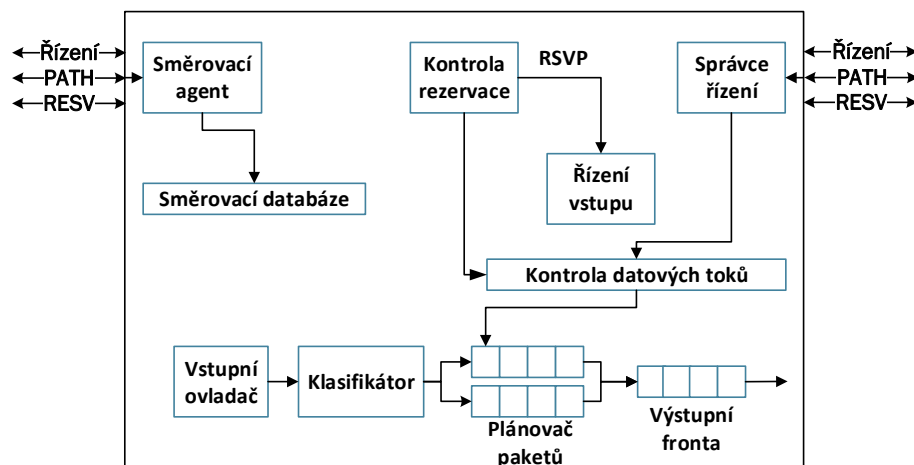


Obr. 2.2: Komunikace pomocí protokolu RSVP. [1]

Řízení provozu

Zajištění požadované kvality služeb je ve směrovačích implementováno pomocí mechanismu, který se nazývá řízení provozu. Části, ze kterých se tento mechanismus skládá, jsou klasifikátor a plánovač paketů. V případě, kdy směrovač nebo koncová stanice obdrží žádost v podobě paketu RSVP, je pomocí řízení provozu určeno, zdali dané zařízení vyhovuje požadavkům k dosažení požadované kvality služeb. Poté je kontrolováno, zdali má uživatel povolení pro vytvoření rezervace. Pokud jsou obě podmínky splněny, dojde k nastavení plánovače paketů a klasifikátoru, které zajistí pro dané služby požadovanou kvalitu zacházení. Ale pokud není jedna z podmínek splněna, je rezervace zamítnuta. Pro případ, že existuje více odesílatelů v jedné relaci, existují dva režimy rezervace:

- Sdílená rezervace: rezervace je vytvořena pro určitou skupinu odesílatelů,
- Odlišná rezervace: pro každého uživatele je vytvořena odlišná rezervace.



Obr. 2.3: Řízení provozu mechanismu IntServ. [1]

2.2 Mechanismus Diferencovaných služeb (DiffServ)

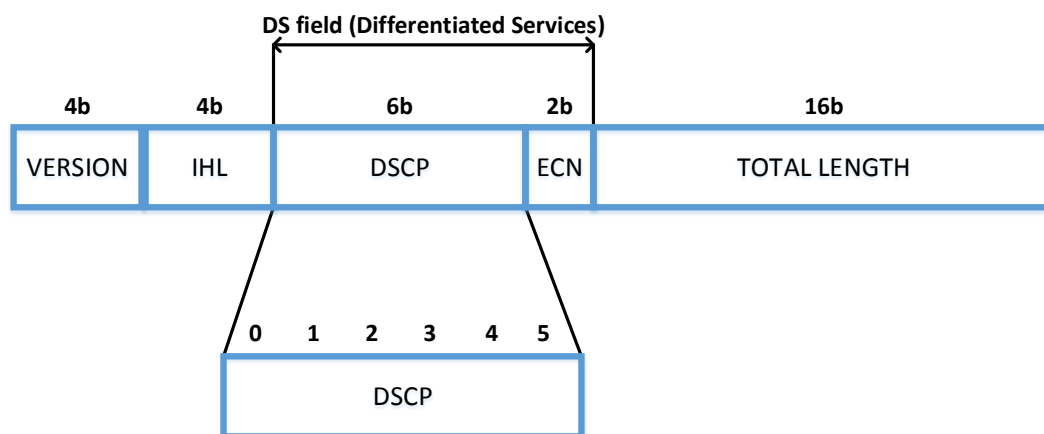
Mechanismus Diferencovaných služeb dělí služby v síti podle jejich požadavků na přenos. Každá služba je přiřazena do určité třídy. Směrovače pak s každou třídou zacházejí odlišně. Odlišného zacházení pro jednotlivé třídy je dosaženo pomocí řízeného přidělování síťových zdrojů. Používá se jak v lokálních tak i v páteřních sítích. V dnešní době se mechanismus DiffServ (Differentiated Services) používá téměř v každé síti, kde je požadováno rozdílné zacházení s jednotlivými službami. Svým provozem nezatěžuje hardware směrovačů v takovém měřítku jako mechanismus IntServ. Veškeré funkce mechanismu DiffServ jsou popsány v RFC 2475 [11].

2.2.1 Značkování paketů

V mechanismu DiffServ proces značkování neudává význam o absolutní prioritě paketu, jako tomu bylo původně u pole ToS, ale určuje identifikátor třídy. Značkováním paketu tak dojde k jeho zařazení do určité třídy. Pro identifikaci třídy se nastavuje hodnota pole DSCP, které se v protokolu IPv4 nachází v hlavičce IP datagramu. Ke značkování dochází na hraničních směrovačích v DiffServ doméně, která je popsána v kapitole 3. Páteční směrovače pakety už neznačkují, pouze s nimi zacházejí podle hodnoty pole DSCP. Pakety, které vstupují do směrovače, už mohou být označovány jiným prvkem sítě. Pokud už pakety byly označovány, daný směrovač je může přeznačit. K přeznačování dochází, když pakety vybočují z předem sjednaných parametrů přenosu. Dalším důvodem přeznačování může být situace, kdy pakety přichází ze sítě, kde se používají odlišná pravidla značkování. U protokolu IPv6 jsou značky mechanismus DiffServ vkládány do pole třídy provozu, tzv. Traffic Class. [2]

Differentiated Service Code Point (DSCP)

V mechanismu DiffServ se pole ToS označuje DS, podle anglického názvu Differentiated Services. Specifikace tohoto pole je uvedena v dokumentu RFC 2474 [8], který byl poté upraven dokumentem RFC 3260 [12]. Jak už bylo uvedeno, pole DS neudává význam o absolutní prioritě paketu, jako tomu bylo původně u pole ToS, ale určuje identifikátor třídy. Rozděluje se na dvě další pole. První pole je označováno DSCP a zahrnuje prvních šest bitů, které nesou kódové označení diferencované služby a jsou používány k označení třídy. Zbylé dva bity spadají pod pole ECN (Explicit Congestion Notification). Struktura pole DS je na obr. 2.4.



Obr. 2.4: Struktura pole DS podle [13].

Nejvýznamnějším bitem je levý krajní bit. Naopak pravý krajní bit má nejmenší význam. Protože pole DSCP obsahuje šest bitů, lze vytvořit celkem 64 různých hodnot. Kvůli kompatibilitě s polem ToS a jeho částí IP Precedence je zavedeno osm tříd, které jsou označeny zkratkou CS0 až CS7 (Class Selector – CS). Jednotlivé třídy se rozlišují na základě hodnoty prvních tří bitů. Obecně platí, že do třídy z větší hodnotou se přiřazují služby, které kladou větší požadavky na přenos. Nastavení zbývajících tří bitů je na správci sítě. Základní rozdělení tříd je znázorněno v tab. 2.1.

Tab. 2.1: Základní rozdělení tříd podle hodnoty pole DSCP. [14]

Třída	IP Precedence	DSCP
CS7	7	111 000
CS6	6	110 000
CS5	5	101 000
CS4	4	100 000
CS3	3	011 000
CS2	2	010 000
CS1	1	001 000
CS0	0	000 000

Dále je zaveden způsob zacházení s pakety dané služby, tzv. Per-Hop Behavior – PHB. Dochází k rozdělení třídy CS1 až CS5 na další podtřídy, které jsou uvedeny v tab. 2.2. Způsob zacházení s pakety PHB může být definován pomocí šířky pásma, velikostí vyrovnávacích pamětí, způsobem zacházení vůči jiným PHB nebo parametry provozu jako je zpoždění, kolísání zpoždění a ztrátovost. Jsou specifikovány tři základní způsoby zacházení.

Standardní PHB (Best-Effort – BE)

Poskytuje službu Best-Effort. Standardní PHB dostane nejnižší prioritu a podle toho je s pakety zacházeno. Má tedy snahu doručit co nejvíce paketů v nejkratší době. Doporučené DSCP je 000 000. Pakety tedy nejsou zařazeny do žádné z definovaných tříd. [1]

Zajištění předávání (Assured Forwarding – AF)

Způsob AF je určen především pro služby, které kladou důraz na spolehlivost. Jinými slovy je kladen důraz na co nejmenší ztrátovost paketů. Zaručením větší spolehlivosti dojde k většímu zpoždění a k výraznějšímu kolísání zpoždění. Rozděluje se na čtyři třídy, které mají stejnou hodnotu prvních tří bitů pole DSCP jako třídy

CS1 až CS4. Rozdíly mezi třídami závisí na přiřazení určité části šířky pásma. Dané rozdělení provádí správce sítě. Třídy se dále dělí na tři podtřídy, které určují pravděpodobnost zahození paketu při zatížení směrovače. Každé podtřídě je přidělena priorita. Pakety z podtřídy o nejnižší prioritě budou zahozeny s nejmenší pravděpodobností. Naopak pakety z podtřídy o nejvyšší prioritě budou zahozeny s největší pravděpodobností. Pakety jsou rozděleny do podtříd na základě měření příchozího provozu. Pokud příchozí paket splňuje sjednanou rychlost, pak je zařazen do podtřídy s nejnižší pravděpodobností zahození. Naopak při překročení sjednané rychlosti jsou pakety zařazeny do podtřídy s nejvyšší pravděpodobností zahození. Do podtřídy s větší pravděpodobností zahození jsou pakety zařazeny, pokud přesahují sjednanou rychlost, ale jen v krátkodobých tolerovaných limitech. Podrobný popis zacházení způsobem AF je v dokumentu RFC 2597 [15], který byl upraven dokumentem RFC 3260 [12].

Urychlené předávání (Expedited Forwarding – EF)

Služby, které kladou důraz na zpoždění a kolísání zpoždění při nízké ztrátovosti, jsou určeny pro tento způsob zacházení PHB. Jedná se tedy o služby pracující v reálném čase. Způsob EF není rozdělen na čtyři podtřídy, jako tomu bylo u způsobu AF. Zahrnuje pouze jednu třídu, která má větší prioritu než všechny ostatní třídy AF a Best-Effort. Hodnota prvních tří bitů pole DSCP odpovídá třídě CS5. Nejvyšší priorita byla této třídě přidělena, aby bylo možné pakety obsloužit přednostně, čímž jsou dodrženy přísné požadavky na zpoždění a kolísání zpoždění. Pro dodržení těchto požadavků je také důležité přidělení určité části šířky pásma pro danou třídu. Protože se jedná o jednu třídu, do které jsou vkládány pakety služeb, které kladou důraz na minimální zpoždění a kolísání zpoždění, měla by být šířka pásma přidělena až po analýze provozu. Způsob zacházení EF byl poprvé specifikován v RFC 2598 [16]. Další specifikace je obsažena v dokumentu RFC 3264 [17].

Tab. 2.2: Rozdělení tříd podle hodnoty pole DSCP v závislosti na PHB. [18]

Třída	Značení třídy	IP Precedence	DSCP	Hodnota	Služby
CS7	CS7	7	111 000	56	směrovací protokoly v lokální síti
CS6	CS6	6	110 000	48	směrovací protokoly
CS5	EF	5	101 110	46	hlasové služby
	CS5		101 000	40	
CS4	AF43	4	100 110	38	videokonference
	AF42		100 100	36	
	AF41		100 010	34	
	CS4		100 000	32	
CS3	AF33	3	011 110	30	uživatelsky kritické služby
	AF32		011 100	28	
	AF31		011 010	26	
	CS3		011 000	24	
CS2	AF23	2	010 110	22	transakční a interaktivní služby
	AF22		010 100	20	
	AF21		010 010	18	
	CS2		010 000	16	
CS1	AF13	1	001 110	14	objemná data
	AF12		001 100	12	
	AF11		001 010	10	
	CS1		001 000	8	
CS0	BE	0	000 000	0	data nevyžadující vysokou prioritu Best-Effort

Rozdíl mezi třídami EF, AF1–AF4 a BE je v prvních třech bitech pole DSCP. Dané tři bity jsou zároveň používány i v poli ToS pro určení jedné z osmi priorit. Pro shodné hodnoty pole DSCP a IP Precedence je přiřazena stejná služba. Vzájemná kompatibilita pole DSCP a pole ToS je patrná i z hodnot dalších třech bitů. Například aplikací hlasové služby na obě pole. Jak bylo uvedeno v kapitole 1.2, hlasové služby kladou důraz hlavně na zpoždění. To znamená, že v poli ToS by byl nastaven čtvrtý a pátý bit do stavu logické jedničky. Zároveň je známo, že pro hlasovou službu je doporučeno nastavit pátou prioritu. Takže v binárním vyjádření by pole ToS, pro hlasovou službu, bylo 101 110. V případě DSCP patří hlasová služba do třídy EF. Tato třída má v binárním zápisu hodnotu 101 110, která je stejná jako pro pole ToS.

2.2.2 Klasifikace paketů

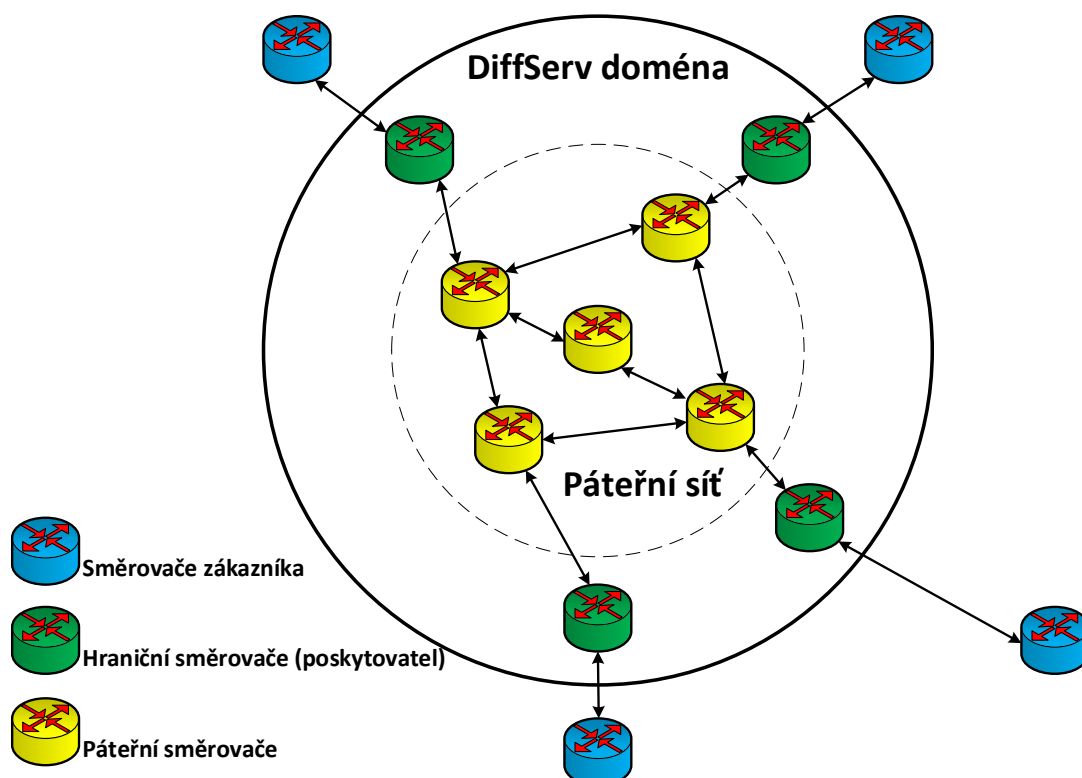
Procesem klasifikace se jednotlivé pakety rozdělují do skupin podle předem stanovených pravidel. Klasifikace probíhá na základě procesu značkování. Pokud jsou příchozí pakety označovány, jsou na základě značky rozděleny do skupin. V případě, že jsou příchozí pakety neoznačovány, dojde k jejich označení po klasifikaci. Rozdělení paketů do skupin se provádí na základě libovolného identifikátoru, který byl paketu přidělen při značkování. Identifikátor je informace uložená v hlavičce datové jednotky. U metody DiffServ je identifikátorem hodnota pole DSCP, kde její hodnota udává třídu, do které paket patří. Mezi dva základní procesy klasifikace patří sloučené vyhodnocování, tzv. BA – Behaviour Aggregate, a vícepoložkové třídění, tzv. MF – Multi-Field Classification. [2]

Sloučené vyhodnocování BA řadí pakety do tříd na základě jediného identifikátoru. Tímto identifikátorem je značka v hlavičce IP paketu v poli DSCP. Klasifikace BA se používá, pokud paket, který přichází na směrovač, byl již označen jiným zařízením. Tato klasifikace se provádí na páteřním směrovači, viz kap. 3.2.

Vícepoložkové třídění MF klasifikuje pakety podle jednoho nebo více identifikátorů. Těmito identifikátory může být zdrojová adresa, cílová adresa, typ protokolu, zdrojový port nebo cílový port. Řazení paketů podle klasifikace MF může být také provedeno na základě kombinace daných identifikátorů. Tato klasifikace se používá na hraničním směrovači (viz kap. 3.1), kde na základě několika parametrů jsou vybrány pakety, které budou následně označovány. Podobně jako pro značkování platí i pro klasifikaci paketů, že pokud byly pakety klasifikovány v jiné části sítě, může hraniční směrovač klasifikaci ponechat nebo změnit.

3 DIFFSERV DOMÉNA

Jedním z hlavních požadavků na mechanismus diferencovaných služeb je, aby aktivní síťové prvky, konkrétně směrovače, nebyly vytíženy zajištěním kvality služeb. Hlavním úkolem směrovače je najít nejvhodnější cestu pro doručení paketů cílovému uzlu. Směrovač také musí mimo jiné udržovat informace o připojených sítích a jejich parametrech. Zajištění kvality služeb je pouze další přídatnou funkcí směrovače. Mezi výpočetně náročnější procesy mechanismu diferencovaných služeb patří klasifikace paketů, značkování paketů a dodržení předem sjednaných parametrů provozu. Řazení paketů do front patří také mezi náročné procesy, ale správa front je nedílnou součástí každého směrovače. Nejedná se o přídatnou funkci. Aby byla zajištěna kvalita služeb s minimálním zatížením směrovačů, bylo nutné zredukovat místa v síti, kde jsou tyto procesy prováděny. Řešením bylo rozdělit jednotlivé procesy diferencovaných služeb mezi směrovače. Došlo tak k rozdělení na hraniční a páteřní směrovače, které dohromady zajišťují určitý způsob zacházení s pakety. Část sítě, která je tvořena hraničními a páteřními směrovači, se nazývá DiffServ doména. Model DiffServ domény je znázorněn na obr. 3.1. [2]

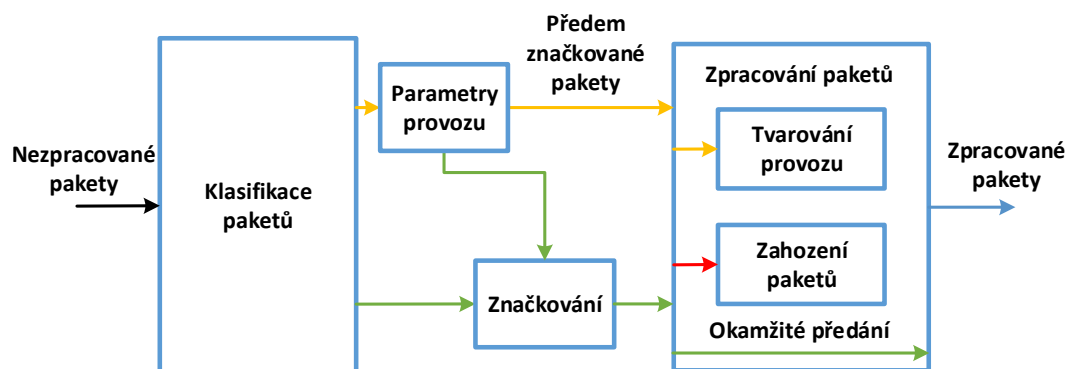


Obr. 3.1: Model DiffServ domény. [2]

Do hraničního směrovače poskytovatele služby přicházejí pakety, které jsou obecně vnímány jako neoznačkovány. Paketům je tedy procesem značkování na základě určitých pravidel, které jsou kontrolovány procesem klasifikace, přidělena značka nastavením pole DSCP. Nakonec jsou paketům přiděleny sjednané parametry provozu. Na vstupní rozhraní páteřního směrovače pak pakety přicházejí označkovány. Pakety projdou procesem klasifikace a následně dojde k jejich rozdělení do front. Detailnější popis zpracování paketů na hraničním a páteřním směrovači je uveden v následujících kapitolách. [19]

3.1 Hraniční směrovač

Hraniční směrovač provádí výpočetně náročnější operace pro zajištění kvality služeb pomocí DiffServ mechanismu. Musí tak být schopen značkovat a klasifikovat pakety příchozího datového toku, ale také kontrolovat a dodržovat sjednané parametry provozu. Zjednodušený princip obsluhy operací mechanismu diferencovaných služeb v hraničním směrovači je zobrazen na obr. 3.2. Jedná se pouze o teoretický model.



Obr. 3.2: Postup zpracování paketů v hraničním směrovači. [2]

Na vstupu směrovače jsou nejdříve pakety klasifikovány. Na základě klasifikace jsou pakety označovány, ale pokud jsou příchozí pakety již označovány, dojde pouze ke kontrole sjednaných parametrů provozu. Pokud parametry nejsou dodrženy, jsou pakety přeznačovány. Následně projdou pakety procesem zpracování, kde dochází k tvarování provozu nebo k zahození paketů. Popsané procesy se dějí na vstupu směrovače. Dále jsou zpracované pakety ve směrovači předány dalším procesům, kde se rozhodne o jejich odeslání.

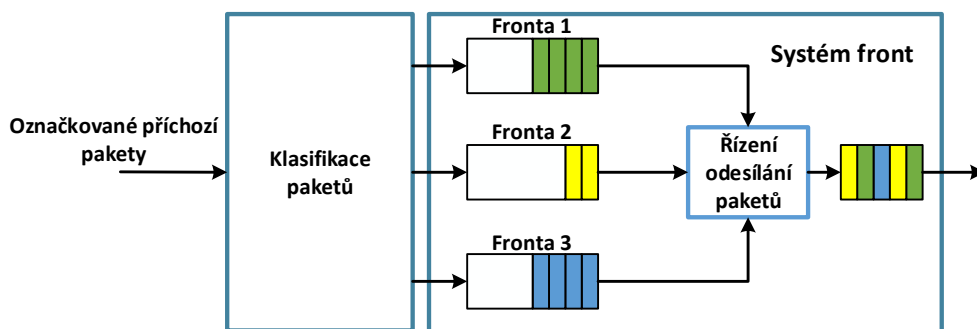
Existují dvě možnosti, mezi kterými sítěmi se může hraniční směrovač nacházet. Jednou z možností je, že hraniční směrovač propojuje dvě sítě, kde jedna z nich me-

chanismus diferencovatelných služeb podporuje a druhá mechanismus nepodporuje. V takovém případě se může jednat o směrovač poskytovatele služby, jak je znázorněno na obr. 3.1. Pakety tedy přicházejí neoznačované a směrovač musí zajistit jejich označkování. Hraniční směrovač také může propojovat jenom sítě s podporou mechanismu diferencovaných služeb. Uvedme příklad, kde jsou dvě DiffServ domény, které jsou propojeny hraničním směrovačem. Při komunikaci mezi těmito doménami mohou nastat dva případy obsluhy paketů. V prvním případě jsou sjednané parametry provozu v obou doménách odlišné. Potom pakety, které jsou přes hraniční směrovač přeposlány z jedné domény do druhé, budou přeznačkovány. V druhém případě, kdy jsou sjednané parametry provozu stejné nebo velice podobné a pakety jsou již označkovány, budou pakety po klasifikaci předány ke zpracování.

Pro zpracování výpočetně náročnějších operací na hraničním směrovači existují dva hlavní důvody. Za prvé jsou páteřní směrovače více vytížené síťovým provozem a za druhé je výhodné, aby nastavení požadovaných parametrů pro zajištění kvality služeb bylo provedeno hned po odeslání nově vytvořeného datového provozu.

3.2 Páteřní směrovač

Páteřní směrovače tvoří spoje mezi hraničními směrovači. Příchozí pakety jsou již označkovány. Z hlediska diferencovaného zacházení jsou příchozí pakety nejdříve klasifikovány a podle hodnoty pole DSCP rozděleny do příslušných front dané priority. Specifikace prioritního systému front je uvedena v kapitole 4. Rozdělením do front je paketům přidělena určitá část šířky pásma a určitá část zpoždění pro jednotlivé třídy, do kterých pakety patří. Záleží také na implementovaném systému front. Zjednodušený princip obsluhy operací mechanismu diferencovaných služeb v páteřním směrovači je na obr. 3.3. Jedná se pouze o teoretický model.



Obr. 3.3: Postup zpracování paketů v páteřním směrovači. [2]

4 SYSTÉMY FRONT

Jedním ze způsobů zajištění kvality služeb na směrovačích je proces řazení paketů do oddělených front. Tento proces se provádí na páteřních směrovačích v rámci DiffServ domény. Odesílání paketů závisí na použitém systému front a jeho nastavení. Každý systém front přiřazuje každé frontě prioritu. Výjimku tvoří pouze fronta typu FIFO, protože obsahuje pouze jednu frontu. Obecně platí, že pakety z fronty s větší prioritou jsou odeslány jako první. Jaká priorita je danému paketu přiřazena, neboli do jaké fronty je paket zařazen, rozhodne proces klasifikace na základě třídy, do které paket patří. Velmi důležitým úkolem je také dohled nad síťovými prostředky, především nad šířkou pásma, která by měla být mezi jednotlivé fronty rozdělena spravedlivě. Používají se ale i systémy front, které upřednostňují šířku pásma pro fronty s větší prioritou. Potom pakety ve frontách s nižší prioritou jsou pozdrženy až do doby, kdy jsou fronty s vyšší prioritou prázdné. Existuje sedm základních systémů front:

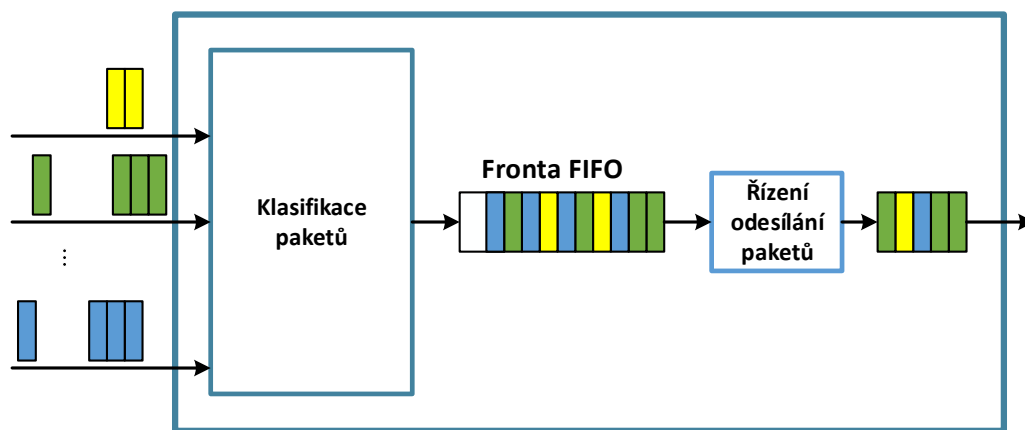
- systém fronty typu FIFO (First In First Out),
- prioritní systém front (Priority Queuing – PQ),
- systém front se spravedlivou obsluhou (Fair Queueing – FQ),
- systém front s váženou cyklickou obsluhou (Weighted Round Robin – WRR),
- systém front s váženou spravedlivou obsluhou (Weighted Fair Queueing – WFQ),
- systém založený na třídách s váženou spravedlivou obsluhou (Class-Based Weighted Fair Queueing – CB WFQ),
- systém založený na třídách s prioritní frontou (Low Latency Queuing – LLQ).

Směrovač obecně pro každý systém front používá stejný postup zpracování. Podle směrovací tabulky jsou pakety přivedeny na požadovaný vstupní port. Poté každý vstupní port provede klasifikaci paketů. Na základě této klasifikace pakety zařadí do odpovídající fronty s příslušnou prioritou. Poté mechanismus řízení front určí, ze které fronty bude paket předán na výstup. Pro každý systém front je však mechanismus řízení front odlišný, záleží na jeho konfiguraci. [2]

4.1 Systém fronty typu FIFO

Fronta typu FIFO je výchozí systém front každého směrovače, pokud není implementován žádný jiný systém. Jedná se o jedinou frontu, takže zde není žádný prioritní mechanismus. Pakety v této frontě mají tedy stejnou prioritu, a proto je se všemi pakety zacházeno stejně. Tato vlastnost je největší nevýhodou tohoto systému, protože neumí rozlišit třídy služeb. Funkci tohoto systému je možné odvodit z jeho názvu. Pakety jsou do fronty řazeny v pořadí, v jakém byly přijaty (First In) a ve

stejném pořadí jsou také odeslány (First Out). Velkou výhodou tohoto systému je velice jednoduchá obsluha, protože nevyžaduje žádný speciální algoritmus pro odesílání paketů. Vyhovuje pro síťové technologie typu Best-Effort. Systém fronty typu FIFO je uveden na obr. 4.1.



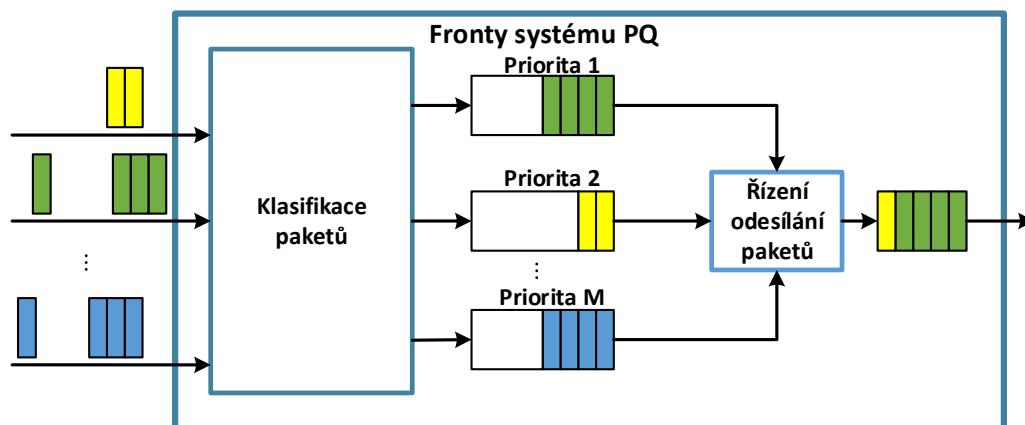
Obr. 4.1: Princip systému fronty typu FIFO. [2]

4.2 Prioritní systém front (Priority Queuing – PQ)

Prioritní systém front obsahuje více front, kde každá fronta má určitou prioritu. Přicházející pakety jsou klasifikovány a následně, podle toho do jaké třídy patří, přiřazeny do fronty o dané prioritě. Odesílání paketů z front je provedeno na základě priority každé fronty. Pakety ve frontě s největší prioritou jsou upřednostněny před pakety ve frontách s nižší prioritou. Takže pakety z fronty o prioritě j jsou odeslány jen v případě, pokud všechny fronty s vyšší prioritou, tj. fronty s prioritou mezi 1 až $j - 1$, jsou prázdné. To znamená, že pokud fronta o nejvyšší prioritě neustále obsahuje pakety k odeslání, pak nikdy nedojde k odeslání paketů z front o nižší prioritě. Možné potlačení odesílání paketů z front nižších priorit je jasná nevýhoda tohoto systému. Naopak výhodou je jednoduchá obsluha, protože používá jednoduchý algoritmus pro odesílání paketů. Prioritní systém front je uveden na obr. 4.2. [20]

Prioritní systém front se dá použít v sítích, kde pakety patřící do třídy s největší prioritou budou obsahovat pouze malou část všech paketů daného provozu v síti. Pak pakety patřící do třídy s nižší prioritou nebudou znevýhodněny při odesílání ze směrovače. Druhou možností efektivního použití prioritního systému je provoz vyžadující přenos v reálném čase. Pakety provozu v reálném čase patří do třídy s největší prioritou.

Z důvodu prevence úplného potlačení provozu a zajištění minimální šířky pásma pro fronty s nižší prioritou se prioritní systém také používá s řízenou rychlostí, tzv. Rate-Controlled PQ. Princip spočívá ve sledování přenosové rychlosti pro provoz odesílaný z fronty s vyšší prioritou tak, aby nepřesáhla předem danou prahovou hodnotu šířky pásma. Jakmile prahovou hodnotu překročí, dojde k odeslání paketů z fronty nižší priority.

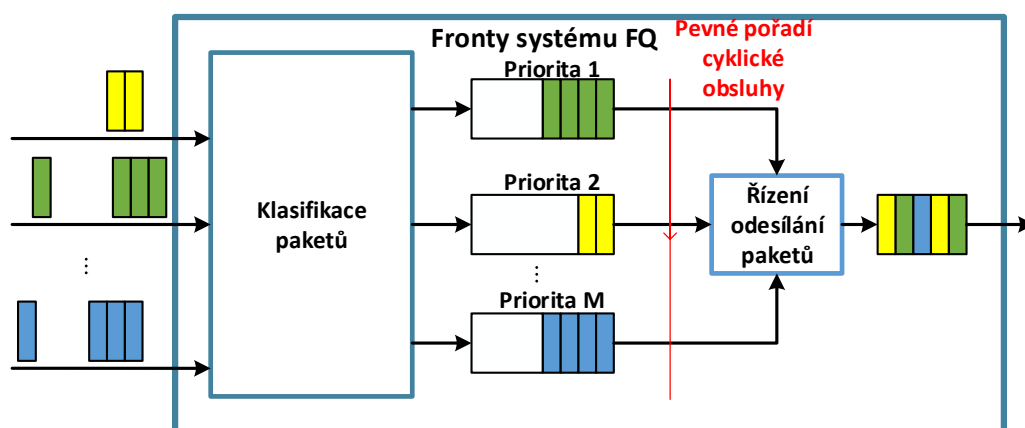


Obr. 4.2: Princip prioritního systému front. [2]

4.3 Systém front se spravedlivou obsluhou (Fair Queuing – FQ)

Systém přijaté pakety řadí do M front. Pro odesílání paketů používá algoritmus round-robin. Pokud fronty obsahují pakety k odeslání, algoritmus během každého cyklu vybere k odeslání maximálně jeden paket z každé fronty. To znamená, že za jeden cyklus je odesláno maximálně M paketů, kde každý paket patří do jiné třídy. Neboli je odesláno maximálně M paketů, kde každý je odeslán z fronty jiné priority. Nejprve je samozřejmě odeslán paket z fronty nejvyšší priority a posledním odeslaným paketem, za jeden cyklus, je paket z fronty s nejnižší prioritou. Systém front se spravedlivou obsluhou je uveden na obr. 4.3.

Systém se spravedlivou obsluhou vyžaduje také jednoduchou obsluhu, protože nepoužívá algoritmus pro alokaci šířky pásma pro jednotlivé fronty. Pokud směrovač přijme paket jiné třídy, než pakety přijaté do této doby, pouze ke stávajícím frontám přidá další frontu.



Obr. 4.3: Princip systému front se spravedlivou obsluhou. [2]

Tento systém však obsahuje dvě velké nevýhody. Každá fronta je obsloužena se stejnou pravidelností. Systém není schopen rozdělit šířku pásma pro jednotlivé fronty. Takže nemůže vyhovět v případě, kdy datové toky jednotlivých front vyžadují odlišné požadavky na šířku pásma. Druhou nevýhodou je, že pakety jsou z jednotlivých front přeneseny jeden po druhém bez ohledu na jejich velikost. Pokud budou dvě fronty, kde je délka paketů stejná, pak je šířka pásma využita spravedlivě. Ale může nastat i případ, kdy je délka paketů ve frontě s nižší prioritou větší jak délka paketů ve frontě s vyšší prioritou. Pak i přes spravedlivou obsluhu obsadí datový tok s větší délkou paketů větší šířku pásma. Tuto nevýhodu dokazuje následující příklad, který byl převzat z [2]. Na rozhraní směrovače jsou přijaty dva datové toky, kde každý obsahuje pakety pro jednu ze dvou front. Fronta A obsahuje první datový tok a má prioritu j . Fronta B obsahuje druhý datový tok a má prioritu k . Mezi prioritami platí vztah $j > k$. První datový tok obsahuje pakety o délce 300 B. Délka paketů druhého datového toku je 800 B. Pak šířka pásma bude procentuálně mezi jednotlivé datové toky rozdělena následovně:

- 1. datový tok:

$$\frac{\text{délka paketu}}{\text{šířka pásma}} \cdot 100 = \frac{200}{200 + 800} \cdot 100 = \frac{200}{1000} \cdot 100 = 20\%,$$

- 2. datový tok:

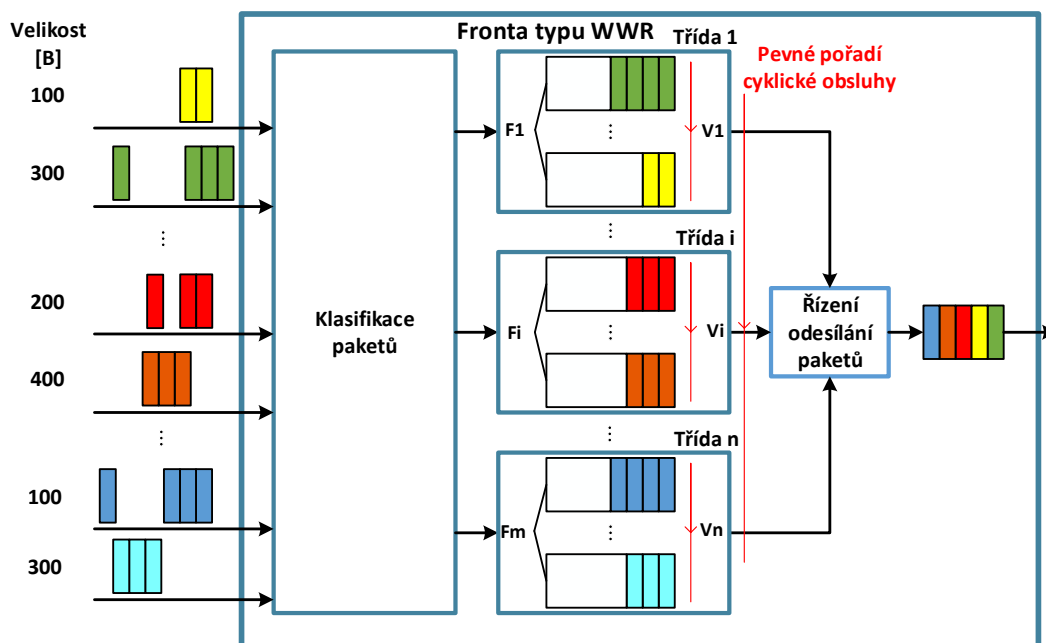
$$\frac{\text{délka paketu}}{\text{šířka pásma}} \cdot 100 = \frac{800}{200 + 800} \cdot 100 = \frac{800}{1000} \cdot 100 = 80\%.$$

Cyklická obsluha front zapříčiní, že paket z fronty o prioritě j je sice odeslán jako první, ale paket z fronty o prioritě k , zabere 80 % šířky pásma. Dochází tedy

k velkému zpoždění mezi odesíláním jednotlivých paketů z fronty A. Pokud datový tok, který zabere pouze 20 % šířky pásma, tvoří služba pracující v reálném čase, dojde k degradaci její kvality.

4.4 Systém front s váženou cyklickou obsluhou (Weighed Round Robin – WRR)

V některých odborných literaturách se můžeme setkat s označením jako řízení front podle třídy, tzv. Class-Based Queuing – CBQ. Systém WRR je schopen pro jednotlivé třídy zajistit požadovanou šířku pásma. Nejprve jsou pakety klasifikovány a následně rozděleny do n tříd, kde první třída má největší prioritu a poslední třída má prioritu nejmenší. Dále jsou pakety v rámci každé třídy rozděleny do m front. Ke každé třídě je přiřazena váhová hodnota V_n , která vyjadřuje procentuální využití šířky pásma. Součet všech váhových hodnot musí být roven 100 %. Pro předání paketů na výstup se používá dvouúrovňové cyklické plánování round-robin. Pokud bude váha první třídy například rovna 20 %, pak cyklická obsluha stráví právě 20 % času odesíláním paketů z této třídy. Princip systému front s váženou cyklickou obsluhou je zobrazen na obr. 4.4. [2]



Obr. 4.4: Princip systému front s váženou cyklickou obsluhou. [2]

Jakým způsobem se rozděluje šířka pásma pro jednotlivé datové toky, ukazuje následující příklad, který byl převzat z [2]. Datový provoz je znázorněn na obr. 4.4. Na směrovač přichází šest jednotlivých datových toků, pro které jsou v bajtech uvedeny velikosti jednotlivých paketů. Dále jsou pakety datových toků rozděleny do třech tříd. Každá třída obsahuje dvě fronty. Šířka pásma pro jednotlivé třídy je rozdělena následovně: $V_1 = 50\%$, $V_2 = 30\%$, $V_3 = 20\%$. Mezi fronty v třídách by měla být šířka pásma rozdělena rovnoměrně. Například fronty v první třídě by měly mít přiřazeno 25 % šířky pásma. Protože ale jednotlivé pakety mají odlišnou velikost, bude skutečné rozdělení jiné. Jaké tedy bude skutečné rozdělení, ukazují následující výpočty:

- 1. datový tok:

$$\frac{\text{délka paketu}}{\text{délka datového toku třídy 1}} \cdot V_1 = \frac{100}{100 + 300} \cdot 50 = \frac{100}{400} \cdot 50 = 12,5\%,$$

- 2. datový tok:

$$\frac{\text{délka paketu}}{\text{délka datového toku třídy 2}} \cdot V_1 = \frac{100}{100 + 300} \cdot 50 = \frac{300}{400} \cdot 50 = 37,5\%,$$

- 3. datový tok:

$$\frac{\text{délka paketu}}{\text{délka datového toku třídy 3}} \cdot V_2 = \frac{100}{200 + 400} \cdot 30 = \frac{200}{600} \cdot 30 = 10\%,$$

- 4. datový tok:

$$\frac{\text{délka paketu}}{\text{délka datového toku třídy 4}} \cdot V_2 = \frac{100}{200 + 400} \cdot 30 = \frac{400}{600} \cdot 30 = 20\%,$$

- 5. datový tok:

$$\frac{\text{délka paketu}}{\text{délka datového toku třídy 5}} \cdot V_3 = \frac{100}{100 + 300} \cdot 20 = \frac{100}{400} \cdot 20 = 5\%,$$

- 6. datový tok:

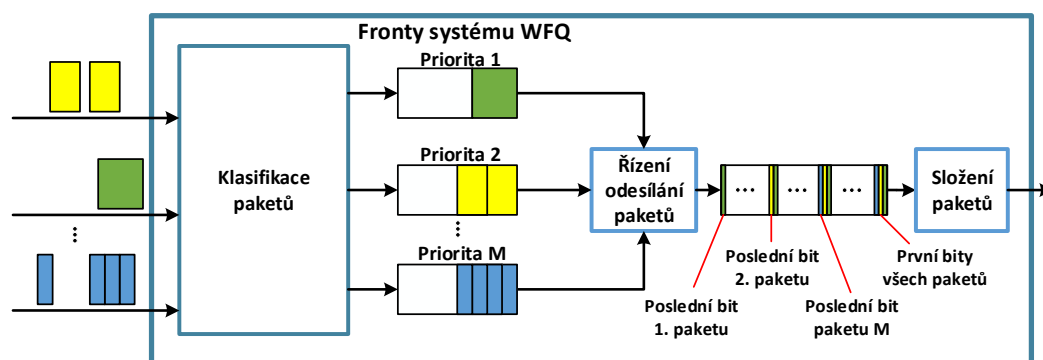
$$\frac{\text{délka paketu}}{\text{délka datového toku třídy 6}} \cdot V_3 = \frac{100}{100 + 300} \cdot 20 = \frac{300}{400} \cdot 20 = 15\%.$$

Z výpočtů je patrné, že druhý datový tok zabere největší část celkové šířky pásma oproti ostatním datovým tokům. Tím tak systém WRR částečně řeší nedostatky systému FQ, kde pakety patřící do stejné třídy zaberou stejnou šířku pásma.

4.5 Systém front s váženou spravedlivou obsluhou (Weighted Fair Queuing – WFQ)

Systém front s váženou spravedlivou obsluhou je schopný eliminovat problém spočívající ve vlivu délky paketů na šířku pásma, který systém WRR nedokázal vyřešit.

Pakety jsou po klasifikaci rozděleny do front. Podobně jako u systému WRR je jednotlivým frontám přidána váhová hodnota určující procentuální využití šířky pásma. Oproti systému WRR zde nejsou fronty děleny do tříd. Rozdělení front je stejné jako u systému FQ. V případě systému FQ byl paket odeslán bez ohledu na jeho velikost. Systém WFQ problém s různou velikostí jednotlivých paketů vyřešil pomocí teoretického modelu cyklické obsluhy. V teoretickém modelu si můžeme představit, že jsou pakety na výstup posílány v určitých blocích, např. bit po bitu. Zpětné sestavení paketů se děje v bloku *složení paketů*. Pakety s větší velikostí se budou skládat déle, proto tedy i jejich odeslání na výstup bude trvat déle. Pakety s menší velikostí mohou být odeslány dříve, ale záleží také na rozdělení šířky pásma pro jednotlivé fronty. Proto se tento systém nazývá se spravedlivou obsluhou, ale spravedlivé je zde pouze respektování velikostí paketů. Důležité je nastavení tohoto systému. Pokud pakety s největší prioritou budou mít největší velikost a vyhrazenou malou šířku pásma, pak jejich předání na výstup bude trvat nejdelší dobu. Proto je důležité posoudit vyhrazení jednotlivých vah pro šířku pásma a také pro jaký datový provoz je vhodné tento systém použít. Princip systému s teoretickým modelem bitové cyklické obsluhy je zobrazen na obr. 4.5. [20]

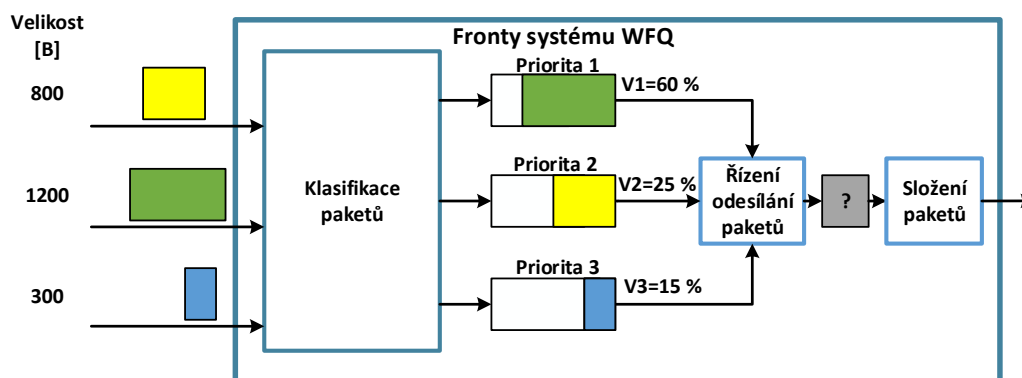


Obr. 4.5: Princip systému front s teoretickým modelem bitové cyklické obsluhy. [2]

Jak můžeme vidět, tak bity jednotlivých paketů jsou odeslány postupně za sebou jako u FQ, ale tento případ nastane jen v případě, kdy váhy rozdělující šířku pásma budou pro všechny fronty stejné.

Pro lepší pochopení systému WFQ je uveden následující příklad podle obr. 4.6, který byl inspirován příkladem z [2]. Ve třech frontách jsou uloženy tři pakety následující velikosti: 1. paket o velikosti 800 B, 2. paket o velikosti 1200 B a 3. paket o velikosti 300 B. Fronta, do které je přiřazen 1. paket, má vyhrazenou šířku pásma 60 %. Pro druhou a třetí frontu jsou vyhrazeny šířky pásma 25 % a 15 %. Pro lepší představu o pořadí, ve kterém budou pakety předány na výstup, si můžeme

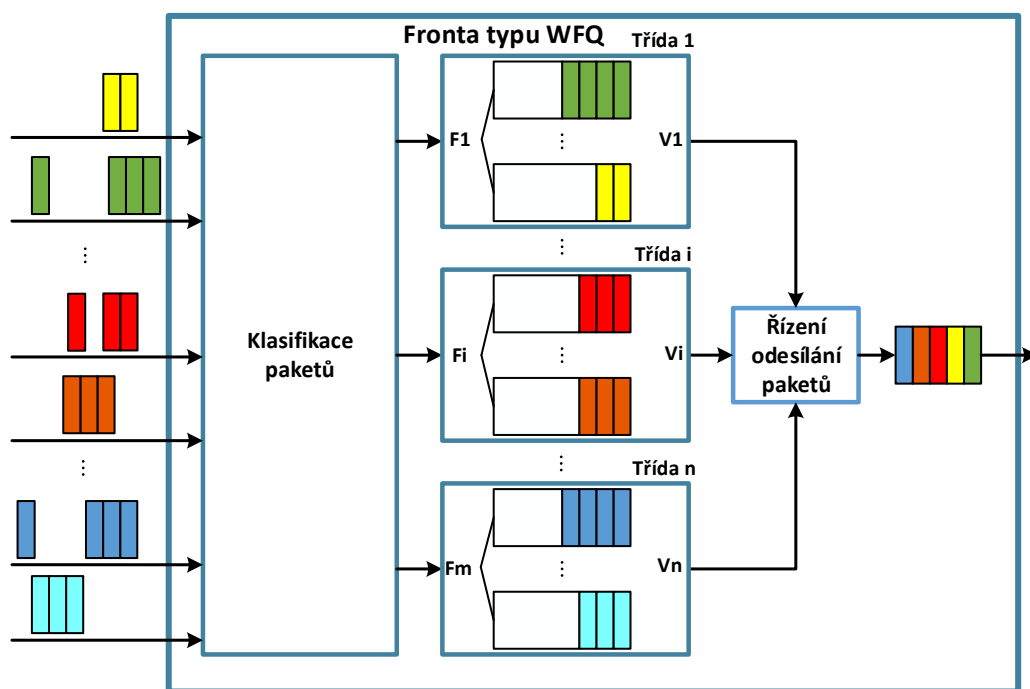
představit, že cyklická obsluha například vybere v každém cyklu 15 B z 1. paketu, 25 B z 2. paketu a 60 B z 3. paketu. Velikosti jednotlivých bloků odpovídají procentuálnímu přiřazení šířky pásma jednotlivým frontám. To znamená, že pro předání 1. paketu na výstup bude potřeba 20 cyklů, 2. paketu 32 cyklů a 3. paketu 20 cyklů. Nejdříve budou odeslány 1. a 3. paket, i když 3. paket je ve třídě s nejmenší prioritou. Jako poslední bude odeslán 2. paket.



Obr. 4.6: Ukázka příkladu datového provozu v systému WFQ. [2]

4.6 Systém založený na třídách s váženou spravedlivou obsluhou (Class-Based Weighted Fair Queuing – CB WFQ)

Jedná se o kombinaci systému WRR a WFQ, viz obr. 4.7. Pakety jsou podobně jako u systému WRR rozděleny do n tříd. Poté jsou v každé třídě rozděleny do odpovídajících front. Každé třídě je přidělena váha vyjadřující procentuální vyhrazení šířky pásma. Součet všech váhových hodnot musí být roven 100 % šířky pásma. Hlavní změna oproti systému WRR je v používání obsluhy front. V systému WRR byla použita dvouúrovňová cyklická obsluha. Systém CB WFQ používá pro obsluhu front v rámci každé třídy stejný postup jako systém WFQ.



Obr. 4.7: Princip systému založený na třídách s váženou spravedlivou obsluhou. [2]

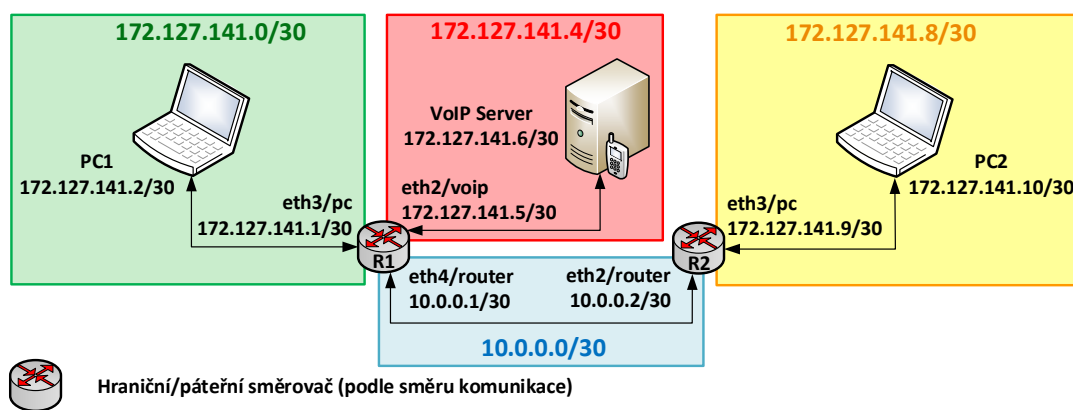
4.7 Systém založený na třídách s prioritní frontou (Low Latency Queuing – LLQ)

Rozdělení front a jejich obsluha je shodná se systémem CB WFQ. Výhodou tohoto systému je možnost vytvoření prioritní fronty jako u systému PQ. Tato fronta je vytvořena na úrovni tříd a bude upřednostněna před ostatními frontami. Frontě je přidělena určitá část šířky pásma a pokud je provozem využita celá šířka pásma, dochází ke kontrole, zdali není překročena přidělená část šířky pásma. Pokud není využita celá šířka pásma, je možné přidělenou část šířky pásma překročit. Tento systém front je vhodné použít, pokud je například potřeba zajistit kvalitní poskytování hlasové služby. [21]

5 NÁVRH LABORATORNÍ ÚLOHY

5.1 Návrh topologie

Topologie laboratorní úlohy je na obr. 5.1. Skládá se ze čtyř sítí. V každé síti se nachází maximálně dvě připojená zařízení. Proto byla v každé síti zvolena maska 255.255.255.252, která v prefixovém tvaru odpovídá hodnotě 30. Sítě jsou navzájem propojeny pomocí dvou směrovačů, které jsou v topologii označeny jako *R1* a *R2*. Na směrovač *R1* je připojená koncová stanice *PC1* a *VoIP server*. Na *VoIP serveru* běží ústředna Asterisk, která slouží pro komunikaci pomocí protokolu SIP (Session Initiation Protocol). Ústředna je nastavená jako proxy server. Ke směrovači *R2* je připojená pouze stanice *PC2*.



Obr. 5.1: Topologie laboratorní úlohy.

5.2 Nastavení koncových stanic a služeb

Pro pochopení funkce QoS byly zvoleny základní služby, se kterými je možné v dnešních datových sítích přijít do styku. Mezi tyto služby patří přenos dat, streamované video a hlasová služba. Aby bylo možné tyto služby testovat, byly na koncové stanice nainstalovány aplikace, které dané služby poskytují.

Přenos dat

Pro přenos dat byla zvolena aplikace *FilleZilla server* a *FilleZilla client*. S názvu je patrné, že aplikace pracují na principu klient-server. Pro přenos dat používají protokol FTP. Protokol FTP spadá pod aplikační vrstvu modelu TCP/IP. Na transportní

vrstvě je používán protokol TCP. Na obou stanicích byl nainstalován server i klient. Na obou serverech je při spuštění vytvořen uživatel, který má nastavené parametry: *Uživatelské jméno: user, Heslo: qosftppc1/qosftppc2 a Sdílená složka: FTP_sdilena*. Pokud je tedy spuštěn server na stanici *PC1*, klient ze stanice *PC2* se přihlásí zadáním údajů: *Hostitel: IP adresa serveru*, v případě *PC1* tedy 172.27.141.2, *Uživatelské jméno: user, Heslo: qosftppc1 a Port: 21*. V případě opačné komunikace probíhá nastavení komunikace stejným způsobem, pouze se změní IP adresa serveru a heslo.

Streamované video

Streamování videa se provádí pomocí aplikace *VLC*. V případě poskytování streamovaného videa stanici *PC1* od stanice *PC2*, musí být nejprve nastavené streamování na stanici *PC2*. Nastavení streamování videa v aplikaci *VLC* je možné v záložce *Média/Proud*, kde se dále možností *Přidat* vybere požadované video. Dále se po vybrání možnosti *proud* vybere protokol *RTP/MPEG Transport stream*. Protokol RTP se používá pro přenos multimediálních dat a spadá pod aplikační vrstvu modelu TCP/IP. Jako transportní protokol je používán protokol UDP. Formát MPEG slouží pro komprimaci videa. Poté se po výběru položky *přidat* nastaví IP adresa stanice, pro kterou je stream vytvořen, v případě *PC1* tedy 172.27.141.2. Port se nechá ve výchozím nastavení 5004. Potvrzením všech dalších nastavení je stream spuštěn. Pro zobrazení streamu je nutné nastavit v programu *VLC*, v záložce *Média/Otevřít síťový proud*, používaný protokol, IP adresu stanice, pro kterou je stream vytvořen, a port. Na stanici *PC1* se tedy zadá *rtp://172.27.141.2:5004*. V případě opačné komunikace probíhá nastavení obdobně, pouze IP adresa se zadá pro stanici *PC2*.

Hlasová služba

Realizace hlasové služby je poskytnuta za pomoci *VoIP serveru* a aplikace *MicroSIP*, která byla nainstalována na obě stanice. Stanice a *VoIP server* mezi sebou komunikují pomocí SIP protokolu, který spadá pod aplikační vrstvu modelu TCP/IP. Jako transportní protokol se používá protokol UDP. Protože je *VoIP server* nastaven jako proxy server, probíhá veškerá komunikace mezi stanicemi přes tento server. Na serveru je možné se zaregistrovat pod číslem 1000 až 1020. V aplikaci *MicroSIP* se tedy pro registraci na daném serveru musela nastavit IP adresa serveru, tj. 172.27.141.6, jedno z daných čísel a heslo, které je stejné jako registrované číslo. Aby datový tok obsahoval co nejvíce dat, byly na každé stanici vytvořeny čtyři účty. Na stanici *PC1* byly nastaveny účty pod čísly 1001, 1002, 1003, 1004 a na stanici *PC2* pod čísly 1017, 1018, 1019, 1020. Pro vytvoření komunikace z *PC1* na *PC2* se zadá na stanici *PC1* jedno z čísel stanice *PC2*. Server pak přijme zprávu, ve které je požadavek: *sip:číslo účtu na stanici PC2/172.27.141.2*. Na serveru je dále vytvořena audio nahrávka,

která je spuštěna po přijetí zprávy s požadavkem *sip:9999/IP adresa volajícího*. Pokud tedy v aplikaci *MicroSIP* je zadáno číslo 9999, je na stanici přijata daná audio nahrávka.

5.3 Konfigurace směrovače R1 a R2


Pro směrování paketů od zdroje k cíli byly vybrány dva RouterBoardy 493G s operačním systémem RouterOS v6.27. Konfigurace směrovačů byla prováděna v grafickém prostředí, které je možné ovládat prostřednictvím aplikace *winbox*. Grafické prostředí RouterOS je znázorněno na obr. 5.2.



Obr. 5.2: Grafické prostředí systému RouterOS v6.27 prostřednictvím aplikace *winbox*.









5.3.1 Nastavení adresace a směrování

VoIP serveru byla přidělena statická IP adresa. Jednotlivá rozhraní obou směrovačů byla přejmenována podle připojeného zařízení. Adresy na jednotlivých rozhraních

směrovačů byly nastaveny staticky v záložce *IP/Address*. Po kliknutí na symbol  se otevře nabídka, kde se zadá IP adresa. Pro přiřazení adres stanicím *PC1* a *PC2* byl nastaven DHCP (Dynamic Host Configuration Protocol) server na rozhraních, ke kterým jsou stanice připojeny. DHCP server je možné nastavit v záložce *IP/DHCP Server*. Dále se vybere nabídka *DHCP Setup*, kde se nastaví rozhraní, na kterém je DHCP server spuštěn, adresní prostor, výchozí brána, adresy, které jsou DHCP serverem přidělovány, DNS server a čas, po který je adresa přidělena. Například při nastavení DHCP serveru na rozhraní *pc* směrovače *R2* byly nastaveny následující parametry:

- rozhraní: *pc*,
- adresní prostor: 172.27.141.8/30,
- výchozí brána: 172.27.141.9,
- přidělované adresy: 172.27.141.10,
- DNS server: 8.8.8.8,
- čas přidělování: 01:00:00.

Aby stanice mezi sebou mohly komunikovat, bylo potřeba na směrovačích nastavit směrování mezi sítěmi. Protože se jedná o jednoduchou topologii, byla zvolena statická konfigurace, která byla prováděna v záložce *IP/Routes*. Například aby mohla komunikovat stanice *PC1* se stanicí *PC2*, bylo na směrovači *R1* nastaveno pravidlo, že pokud směrovač přijme paket s cílovou IP adresou ze sítě 172.27.141.8/30, pošle ho na adresu směrovače *R2*, tj. 10.0.0.2. Obdobné nastavení bylo provedeno na směrovači *R2*. Směrovací tabulky obou směrovačů jsou na obr. 5.3.

R1	Dst. Address	Gateway	R2	Dst. Address	Gateway
DAC	 10.0.0.0/30	router reachable	DAC	 10.0.0.0/30	router reachable
DAC	 172.27.141.0/30	pc reachable	AS	 172.27.141.0/30	10.0.0.1 reachable router
DAC	 172.27.141.4/30	voip reachable	AS	 172.27.141.4/30	10.0.0.1 reachable router
AS	 172.27.141.8/30	10.0.0.2 reachable router	DAC	 172.27.141.8/30	pc reachable

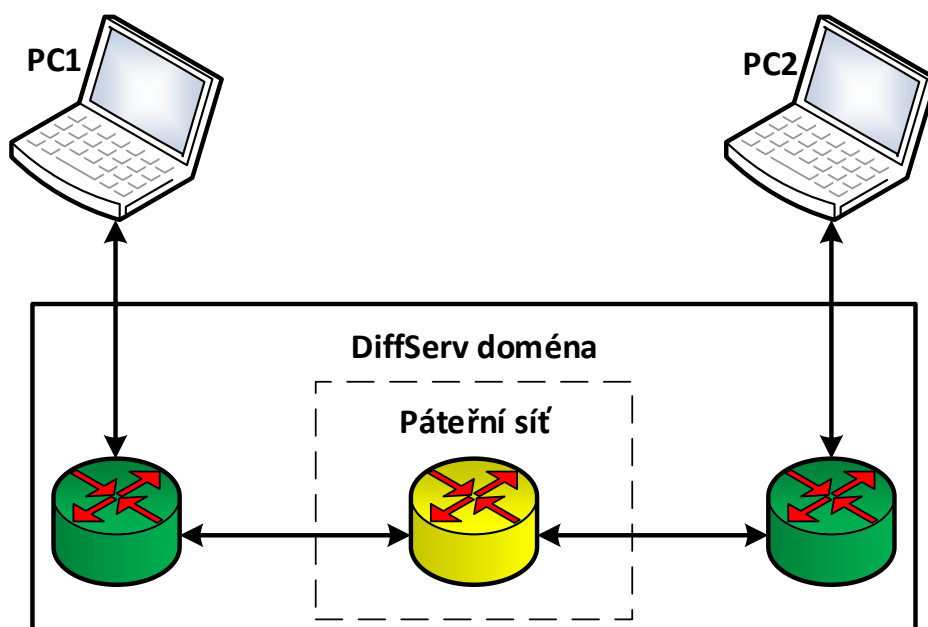
Obr. 5.3: Směrovací tabulky směrovače *R1* a *R2*.

5.3.2 Model DiffServ domény

Pokud požadujeme připojení do sítě, kde je podpora zajištění kvality služeb, musí být připojení provedeno přes hraniční směrovač. Kdybychom byli připojeni přímo na páteřní směrovač, veškerý datový provoz námi vytvořený by nebyl označován. To by mělo za následek, že následující páteřní směrovač by po klasifikaci všechny pakety rozdělil do stejné třídy a se všemi by tak bylo zacházeno se stejnými pravidly. Pokud bychom zároveň například poskytovali službu streamovaného videa a hlasovou službu, mohlo by při zatížení linky dojít k nekvalitnímu poskytování služeb.

Nabízí se jedno řešení, kdy směrovač provádí zároveň procesy hraničního i páteřního směrovače, ale jak bylo uvedeno v kapitole 3, páteřní směrovače jsou více vytíženy z hlediska směrování paketů. Proto byly jednotlivé procesy mechanismu DiffServ rozděleny mezi směrovače.

V laboratorní úloze byl model DiffServ domény zvolen, aby bylo využito co nejméně směrovačů. Model DiffServ domény je uveden na obr. 3.1. Z hlediska ověření funkce DiffServ domény není důležité využití směrovače zákazníka, proto vytvoření jednoduchého modelu DiffServ domény, přes kterou jsou propojeny dvě koncové stanice, je možné pomocí tří směrovačů. Zjednodušený model DiffServ domény je znázorněn na obr. 5.4. Dva směrovače plní funkci hraničních směrovačů, aby odchozí provoz od obou stanic byl klasifikován a označován. Mezi těmito směrovači je pak páteřní směrovač, který pakety klasifikuje a rozděluje do front.



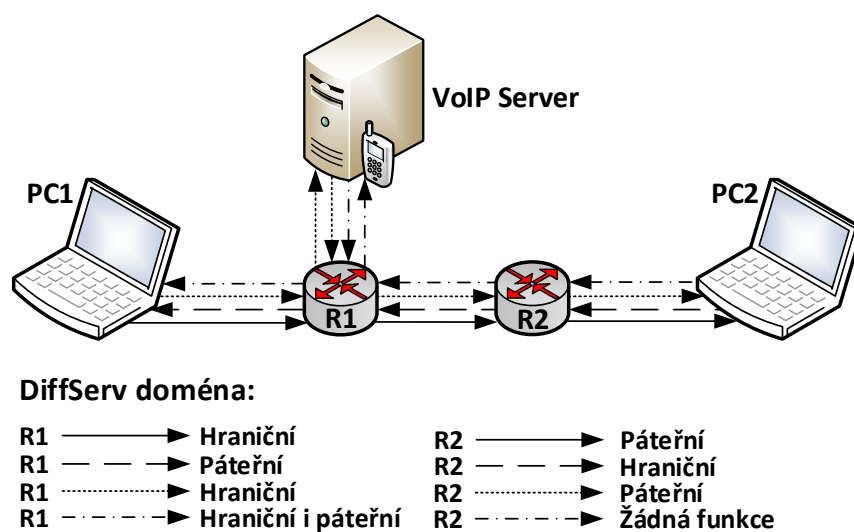
Obr. 5.4: Zjednodušený model DiffServ domény.

Po důkladné analýze možné konfigurace RouterBoardů došlo k rozhodnutí, že v případě laboratorní úlohy budou použity pouze dva směrovače, jak je uvedeno na obr. 5.1. Například pokud stanice *PC1* pošle pakety stanici *PC2*, pak směrovač *R1* pakety na základě klasifikace označuje a směrovač *R2* pakety podle dané značky rozdělí do příslušných front. Při opačné komunikaci plní směrovač *R2* funkci hraničního směrovače a směrovač *R1* funkci páteřního směrovače. Žádný ze směrovačů

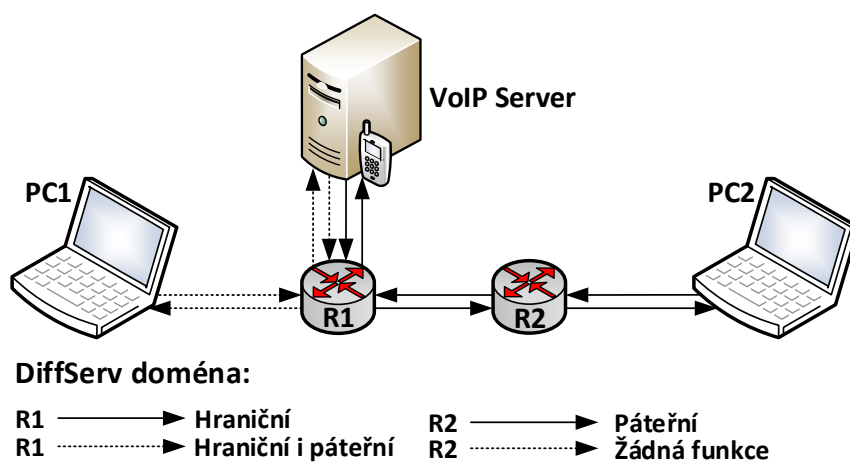
neplní procesy pouze hraničního nebo páteřního směrovače. Záleží na směru komunikace, i když při obousměrné komunikaci dochází na jednom směrovači ke všem procesům mechanismu DiffServ. Dokonce při jednosměrné komunikaci mezi stanicí *PC1* a *VoIP serverem* dochází ke všem procesům, které provádí hraniční i páteřní směrovač. Nicméně v rámci laboratorní úlohy nedochází k velkému vytížení směrovačů z hlediska směrování. Proto nebylo nutné použít tři směrovače, které by odpovídaly ideálnímu modelu DiffServ domény.

Jednotlivé komunikace mezi stanicemi a *VoIP serverem* a nastavení směrovačů jako hraniční nebo páteřní směrovač jsou znázorněny na obr. 5.5, kde obr. 5.5(a) poukazuje na veškerou komunikaci mezi stanicemi *PC1* a *PC2*. Pokud na stanici *PC2* pomocí aplikace MircoSIP zadáme požadavek na navázání hovoru se stanicí *PC1*, bude každý paket přeposílán přes *VoIP server*. Při přenosu dat nebo streamování videa bude komunikace probíhat přímo mezi stanicemi. Jak již bylo výše uvedeno, pro každou komunikaci plní směrovače *R1* a *R2* odlišnou funkci. Při hlasové službě, směrem od stanice *PC1* ke stanici *PC2*, bude směrovač *R1* plnit funkci hraničního směrovače a směrovač *R2* funkci páteřního. V opačném směru, tj. od *PC2* k *PC1*, bude směrovač *R1* plnit funkci hraničního i páteřního směrovače. Dané nastavení, kdy směrovač plní v jednom směru funkci hraničního i páteřního směrovače, je uvedeno v kapitole 5.3.3. Pro poskytování služby přenosu dat nebo streamování videa ve směru od stanice *PC1* ke stanici *PC2*, musí směrovač *R1* plnit funkci hraničního směrovače a směrovač *R2* funkci páteřního směrovače. V opačném směru komunikace se funkce směrovačů *R1* a *R2* prohodí.

Komunikaci mezi *VoIP serverem* a stanicemi znázorňuje obr. 5.5(b). Jedná se o komunikaci, kdy je stanicí *PC1* nebo *PC2* vyslán požadavek na *VoIP server* pro přehrání audio smyčky. Během komunikace směrem od stanice *PC1* nebo *PC2* k *VoIP serveru*, neprovádí směrovače *R1* a *R2* žádný proces DiffServ mechanismu, protože *VoIP server* přijímá pouze pakety hlasové služby. Není tedy nutné pakety v tomto směru rozdělovat do front, když se jedná pouze o jednu a tu stejnou službu. Všechny pakety by byly zařazeny do jediné fronty. Systém o jedné frontě odpovídá frontě FIFO, která je v každém směrovači nastavena jako výchozí. Při komunikaci *VoIP serveru* směrem ke stanici *PC2* plní směrovače *R1* a *R2* stejnou funkci, jako při poskytování hlasové služby směrem od stanice *PC1* ke stanici *PC2*. V případě komunikace *VoIP serveru* směrem ke stanici *PC1* provádí směrovač *R1* procesy hraničního i páteřního směrovače. Směrovač *R2* neprovádí žádný proces. Nastavení směrovačů při této komunikaci odpovídá komunikaci při poskytování hlasové služby směrem od stanice *PC2* ke stanici *PC1*.



(a)



(b)

Obr. 5.5: Možné komunikace mezi stanicemi (a), znázornění komunikace mezi *VoIP serverem* a stanicemi (b).

5.3.3 Nastavení procesů na směrovačích ve funkci hraničního a páteřního směrovače

Aby byla zajištěna správná funkce DiffServ domény, jsou všechny odchozí pakety od koncových stanic a *VoIP serveru* klasifikovány a značkovány na příslušném směrovači. Naopak příchozí pakety, které směřují ke stanicím, musejí být klasifikovány

a na základě klasifikace rozděleny do určité fronty. Pakety směřované přes RouterBoard z jedné sítě do druhé prochází v rámci RouterOS postupně přes řetězec *prerouting*, *forward* a *postrouting*. Procesy klasifikace a značkování na hraničním směrovači jsou nastaveny v řetězci *prerouting*. Stejně tak klasifikace na páteřním směrovači. Výjimku tvoří pouze klasifikace paketů hlasové služby, které jsou určeny pro stanici *PC1*. Tyto pakety jsou klasifikovány v řetězci *forward*. Nastavení procesů na směrovači *R1* a *R2* jsou na obr. 5.6. Pravidla pro klasifikaci a značkování na hraničním směrovači provádějí změnu pole DSCP, jak je uvedeno ve sloupci *Action*. Pro klasifikaci na páteřním směrovači je ve sloupci *Action* uvedeno *mark packet*. Kvůli přehlednosti jsou jednotlivá pravidla pojmenována podle služby a procesu.

R1	Action	Chain	Src. Address	Dst. Address	Protocol	Dst. Port	In. Interface
...	VoIP_PC1_klasifikace_znackovani						
0	✓ change DSCP (TOS)	prerouting	172.27.141.6	172.27.141.2	17 (udp)		voip
...	VoIP_PC2_klasifikace_znackovani						
1	✓ change DSCP (TOS)	prerouting	172.27.141.6	172.27.141.10	17 (udp)		voip
...	VoIP_klasifikace						
2	✗ mark packet	forward		172.27.141.2			voip
...	VLC_klasifikace_znackovani						
3	✓ change DSCP (TOS)	prerouting	172.27.141.2	172.27.141.10	17 (udp)	5004	pc
...	VLC_klasifikace						
4	✗ mark packet	prerouting					router
...	FTP_klasifikace_znackovani						
5	✓ change DSCP (TOS)	prerouting	172.27.141.2	172.27.141.10	6 (tcp)		pc
...	FTP_klasifikace						
6	✗ mark packet	prerouting					router

R2	Action	Chain	Src. Address	Dst. Address	Protocol	Dst. Port	In. Interface
...	VoIP_klasifikace						
0	✗ mark packet	prerouting					router
...	VLC_klasifikace_znackovani						
1	✓ change DSCP (TOS)	prerouting	172.27.141.10	172.27.141.2	17 (udp)	5004	pc
...	VLC_klasifikace						
2	✗ mark packet	prerouting					router
...	FTP_klasifikace_znackovani						
3	✓ change DSCP (TOS)	prerouting	172.27.141.10	172.27.141.2	6 (tcp)		pc
...	FTP_klasifikace						
4	✗ mark packet	prerouting					router

Obr. 5.6: Nastavení procesů hraničního a páteřního směrovače na směrovači *R1* a *R2*.

Nastavení směrovače *R1* ve funkci hraničního směrovače

V kapitole 5.2 bylo uvedeno, že na stanici *PC1* jsou podporovány služby přenosu dat, streamovaného videa a přenosu hlasu, které jsou poskytovány aplikacemi *FilleZilla client* a *server*, *VLC* a *MicroSIP*. Pakety všech těchto služeb, které stanice *PC1* odešle stanici *PC2*, musejí být klasifikovány a označovány na rozhraní *pc* směrovače

R1. Jedinou výjimku tvoří pakety hlasové služby, protože všechny jsou ke stanici *PC2* přeposlány přes *VoIP server*. Proto nejsou tyto pakety klasifikovány a značkovány na rozhraní *pc*, ale na rozhraní *voip*.

Nastavení klasifikace a značkování paketů se provádí v položce *IP/Firewall* (viz obr. 5.2), kde se volí záložka *Mangle*. Přidáním pravidla se otevře okno, kde je možné v záložce *General* a *Advance*, případně *Extra*, nastavit parametry pro proces klasifikace paketů, podle kterých se vyberou pakety, které mají být označovány. Jakým způsobem budou označovány se určí v záložce *Action*. Pro službu přenosu dat jsou pakety klasifikovány podle zdrojové a cílové IP adresy, TCP protokolu a rozhraní *pc*, na kterém jsou pakety od stanice *PC1* přijaty. Zdrojová a cílová IP adresa odpovídá stanici *PC1* a *PC2*. Následně byla v záložce *Action* vybrána možnost *Change DSCP (TOS)*. Hodnota pole DSCP pro službu přenosu dat odpovídá, podle tab. 2.2, hodnotě 14. Uvedená nastavení jsou znázorněna na obr. 5.7. Aplikace *FillZilla client* a *FillZilla server* mezi sebou komunikují pomocí protokolu FTP. Při přihlášení na server používají mezi sebou pro komunikaci port 21, ale při přenosu souboru je používán vždy jiný port z rozsahu 49152–65535. Proto při definování paketů, které se mají označovat, nebyla vybrána možnost portu. V záložce *Action* je možnost *Passthrough*, která určuje, zdali paket po označování prochází i ostatními pravidly. Pokud je možnost vybrána, paket prochází všemi pravidly v záložce *Mangle*. V našem případě je pro pakety jedné služby nastaveno jen jedno pravidlo. Proto tato možnost vybrána není.

Chain:	prerouting
Src. Address:	172.27.141.2
Dst. Address:	172.27.141.10
Protocol:	6 (tcp)
In. Interface:	pc
Action:	change DSCP (TOS)
Log	<input type="checkbox"/>
Log Prefix:	
New DSCP (TOS):	14
Passthrough	<input type="checkbox"/>

Obr. 5.7: Nastavení klasifikace a značkování paketů pro službu přenosu dat.

Nastavení klasifikace a značkování pro službu streamovaného videa je podobné jako pro službu přenosu dat. IP adresy a rozhraní, na kterém jsou pakety značkovány, jsou stejné. Změna je pouze ve transportním protokolu. Pro službu streamovaného videa se používá protokol UDP. V kapitole 5.2 jsme si uvedli, že při nastavení streamování v aplikaci VLC je definován port 5004. Při poskytování streamování videa stanice posílá druhé stanici pakety, kde je nastaven cílový port právě na hodnotu 5004. Aby byly pakety lépe rozeznatelné, byla v definici paketů zahrnuta i položka

cílového portu. V záložce *Action* je hodnota DSCP nastavena opět podle tab. 2.2 na hodnotu 32.

Při určování pravidel pro definici paketů hlasové služby byl nastaven transportní protokol UDP jako u služby streamování videa. SIP protokol však nepoužívá port 5004, ale 5060 nebo 5061. Tento port je použit jen při registraci na serveru, zahajování a ukončení hovoru. Pro samotný přenos hlasu je používán protokol pro podporu multimediálních dat RTP. Při komunikaci pomocí protokolu RTP je používán vždy jiný port než při komunikaci pomocí protokolu SIP. Proto při definování paketů v záložce *General* nebyl zadán žádný port. Změna je také v nastavení rozhraní, na kterém se značkování provádí. Pakety odeslané stanicí *PC1* nemusí být klasifikovány a značkovány. Značkovány musí být pakety vyslané *VoIP serverem*. Proto se klasifikace a značkování provádí na rozhraní *voip*. Také zdrojová IP adresa je nastavena na IP adresu *VoIP serveru*. Hodnota pole DSCP je změněna na hodnotu 46, která odpovídá hodnotě třídy EF.

Pakety jednotlivých služeb jsou tedy klasifikací rozeznatelné na základě používaných transportních protokolů, portů a rozhraní, na kterém se značkování provádí. Je patrné, že při nastavování parametrů procesu klasifikace pro určování paketů je nastavení IP adres i rozhraní, na kterém jsou pakety označovány, zbytečné. Stačilo by nastavit pouze rozhraní. IP adresy slouží hlavně pro lepší orientaci v jednotlivých pravidlech.

Nastavení směrovače R2 ve funkci hraničního směrovače

Na stanici *PC2* jsou podporovány stejné služby jako na stanici *PC1*. Nastavení klasifikace a značkování bude tedy podobné. Rozdíl je pouze v klasifikaci a značkování paketů hlasové služby. Protože pakety určené stanici *PC1* prochází přes *VoIP server*, jsou klasifikovány a značkovány opět na rozhraní *voip* směrovače *R1*. Parametry procesu klasifikace pro výběr paketů hlasové služby jsou stejné, až na cílovou IP adresu, která odpovídá IP adrese stanice *PC1*. Na směrovači *R2* pakety hlasové služby nejsou klasifikovány a tím tedy ani značkovány. To samé platí i v případě komunikace *VoIP serveru* a stanice *PC2*, při požadavku na přehrání audio smyčky.

Klasifikace a značkování paketů služeb přenosu dat a streamovaného videa probíhá stejným způsobem jako na směrovači *R1*. Rozdíl však je v IP adresách, kde zdrojovou IP adresou je IP adresa stanice *PC2* a cílovou je IP adresa stanice *PC1*. Ostatní parametry procesu klasifikace pro definici paketů jsou totožné. Pouze se značkování provádí na rozhraní *pc* směrovače *R2*. Hodnota pole DSCP je také změněna na stejnou hodnotu.

Nastavení směrovače R1 ve funkci páteřního směrovače

Klasifikací musí projít všechny pakety, které jsou určeny pro stanici *PC1*, aby bylo možné pakety rozdělit do front a byla tak zajištěna požadovaná kvalita služeb. Klasifikace se provádí na rozhraní *router* směrovače *R1*. Pouze pakety hlasové služby, které jsou zaslány *VoIP serverem*, jsou klasifikovány na rozhraní *voip*, na kterém jsou také podrobeny procesům hraničního směrovače. Aby směrovač neprováděl procesy hraničního i páteřního směrovače ve stejném řetězci, je proces klasifikace páteřního směrovače prováděn v řetězci *forward*. Nastavení je znázorněno na obr. 5.6 ve sloupci *Chain*. V kapitole 5.3.4 se pak dočteme, že vkládání paketů do front se provádí v *postroutingu*. Takže z pohledu průběhu paketu směrovačem je paket nejprve klasifikován a označován, poté opět klasifikován a nakonec přidělen do určité fronty.

Nastavení klasifikace pro službu přenosu dat je na obr. 5.8. V záložce *General* bylo definováno rozhraní *router*, na kterém se klasifikace bude provádět. Pakety, které jsou určeny pro stanici *PC1*, byly označovány směrovačem *R2*, v případě hlasové služby směrovačem *R1*. Proto bylo nastaveno jediné pravidlo, podle kterého se klasifikace bude provádět. Tím pravidlem je hodnota pole DSCP, která byla nastavena v záložce *Advance*. Konkrétně u paketů služby přenosu dat je hodnota pole DSCP změněna na hodnotu 14. Takže všem paketům, které jsou přijaty na rozhraní *router* a obsahují hodnotu pole DSCP 14, je klasifikací přidělena značka *FTP*, která slouží pro přidělení paketů do příslušné fronty.

The image shows a configuration window for packet classification in Mikrotik WinBox. On the left, under 'Chain', the 'In. Interface' is set to 'router' and 'DSCP (TOS)' is set to '14'. On the right, under 'Action', the 'Action' is set to 'mark packet'. Below this, the 'Log' checkbox is unchecked, and the 'Log Prefix' field is empty. Further down, the 'New Packet Mark' is set to 'FTP', and the 'Passthrough' checkbox is unchecked.

Obr. 5.8: Nastavení klasifikace paketů pro službu přenosu dat.

Klasifikace paketů služby streamovaného videa se provádí stejným způsobem jako u služby přenosu dat. Pouze příchozí pakety mají hodnotu pole DSCP 32. Proto budou vloženy do jiné fronty a bude s nimi zacházeno s jinou prioritou. Po klasifikaci jim bude přidělena značka *VLC* podle aplikace, která službu poskytuje.

Příchozí pakety hlasové služby se klasifikují na rozhraní *voip* a obsahují hodnotu DSCP 46. Po klasifikaci jim bude přidělena značka *VoIP*, podle které s nimi bude

zacházeno. Z teorie služeb a DiffServ mechanismu víme, že s těmito pakety by se mělo zacházet s největší prioritou, ale záleží pouze na charakteru a správci sítě.

Nastavení směrovače R2 ve funkci páteřního směrovače

Nastavení klasifikace je podobné jako na směrovači *R1*. Všechny služby jsou klasifikovány na rozhraní *router*. To platí i pro hlasovou službu, protože *VoIP* server není připojen na tento směrovač. Je připojen přes směrovač *R1*, který je připojen právě na rozhraní *router* směrovače *R2*. Klasifikace opět probíhá na základě hodnoty pole DSCP. Po klasifikaci jsou službám opět přiděleny stejné značky jako na směrovači *R1*, podle kterých jsou rozděleny do front.

5.3.4 Nastavení front

Nastavení front probíhá na směrovačích, které provádí procesy páteřního směrovače. V předchozí kapitole bylo uvedeno, že příchozí pakety směrované jedné ze stanic musí projít procesem klasifikace, ve kterém se na základě hodnoty pole DSCP přidělí paketům značka, podle které budou rozděleny do front. Obsluha front se provádí v řetězci *postrouting*. Na obou směrovačích *R1* i *R2* bylo nastavení provedeno stejným způsobem, proto se dále neuvádí nastavení na konkrétním směrovači.

Základem bylo nastavení jednotlivých systémů front podle teoretického rozboru, který je uveden v kapitole 4. Na obr. 5.9 je zobrazeno nastavení všech systémů. Pouze systém LLQ nebyl zahrnut do konfigurace. Jednalo by se o spojení konfigurace systémů CB WFQ a PQ. Preferování služeb je možné nastavením parametrů *Limit At* a *Max Limit*. Parametr *Limit At* udává minimální garantovanou přenosovou rychlost a *Max Limit* určuje maximální přenosovou rychlost. Parametrem *Max Limit* se tedy nastavuje maximální možná šířka pásma. Samozřejmě pokud je datový tok menší než *Limit At*, bude i přenosová rychlost menší.

Porovnáním nastavení na obr. 5.9, se může na první pohled zdát, že podle těchto parametrů je nejvíce preferovaná služba přenosu dat (FTP), potom streamovaného videa (VLC) a nejméně preferovaná je hlasová služba (VoIP). Preferování služeb je tedy přesně opačné, než jak bylo uvedeno v teoretické části. Ale pokud bychom služby spustili na obou stanicích při neomezeném provozu, zjistíme, že průměrná přenosová rychlost jednotlivých služeb dosahuje následujících hodnot: přenos dat 90 Mb/s, streamované video 400 až 750 kb/s a hlasová služba 320 kb/s. Je tedy patrné, že nejvíce omezená služba je právě přenos dat. Nedochozí k degradaci služby přenosu dat, ale pouze k omezení. Při přenosu dat je používán spolehlivý transportní protokol TCP, který zahozené pakety posílá znovu, dokud nebudou na cílové stanici přijaty. U ostatních služeb při tomto nastavení k degradaci nedochází. Proto následující popis nastavení všech systémů front bude vysvětlen s těmito přenosovými rychlostmi.

Nastavení front se na RouterBoardu provádí v nabídce *Queues*, viz obr. 5.2. Po otevření této nabídky se zobrazí okno, které obsahuje záložky *Simple Queues*, *Interface Queues*, *Queue Tree* a *Queue Types*. Veškerá konfigurace jednotlivých systémů byla prováděna v záložce *Queue Tree*. U systémů front FIFO, PQ, FQ, a WRR byla použita fronta typu *pfifo*, která data odesílá po paketech. Aby byl dodržen teoretický model u systémů WFQ, byla u tohoto systému použita fronta typu *bfifo*, která data odesílá po bajtech. Tento typ fronty byl použit také u systému CB WFQ. Nastavení typu fronty se provádí v záložce *Queue Types*, kde se v případě fronty *bfifo* a *pfifo* zadá pouze velikost fronty v bajtech nebo v paketech.

Name	Parent	Packet Marks	Limit At (bits/s)	Max Limit (bits/s)
CB-WFQ	global			3M
CB-WFQ_FIRST_CLASS	CB-WFQ			1200k
CB-WFQ_VLC	CB-WFQ_FIRST_CLASS	VLC	600k	800k
CB-WFQ_VoIP	CB-WFQ_FIRST_CLASS	VoIP	300k	400k
CB-WFQ_SECOND_CLASS	CB-WFQ			1800k
CB-WFQ_FTP	CB-WFQ_SECOND_CLASS	FTP	1100k	1800k
FIFO	global	FTP, VLC, VoIP	2M	3M
FQ	global			2400k
FQ_FTP	FQ	FTP	600k	800k
FQ_VLC	FQ	VLC	600k	800k
FQ_VoIP	FQ	VoIP	600k	800k
PQ	global			3M
PQ_FTP	PQ	FTP	2100k	3M
PQ_VLC	PQ	VLC	600k	3M
PQ_VoIP	PQ	VoIP	300k	3M
WFQ	global			3M
WFQ_FTP	WFQ	FTP	1100k	1800k
WFQ_VLC	WFQ	VLC	600k	800k
WFQ_VoIP	WFQ	VoIP	300k	400k
WRR	global			3M
WRR_FIRST_CLASS	WRR			1600k
WRR_VLC	WRR_FIRST_CLASS	VLC	600k	800k
WRR_VoIP	WRR_FIRST_CLASS	VoIP	300k	800k
WRR_SECOND_CLASS	WRR			1400k
WRR_FTP	WRR_SECOND_CLASS	FTP	1100k	1400k

Obr. 5.9: Nastavení jednotlivých systémů front.

Fronta typu FIFO

Nastavení fronty je na obr. 5.10. Parametrem *Parent* se uvádí, zdali fronta nespadá pod jinou frontu. V případě nastavení *global* se určí, že fronta je obsloužena v řetězci *postrouting*. V předchozích verzích RouterOS bylo možné vybrat mezi *global-in*, *global-out* a *global-total*, kde každé nastavení znamenalo obsloužení fronty v jiném řetězci. Dalším parametrem je *Packet Marks*, kde se definují pakety služeb, které budou do fronty zařazeny. Procesem klasifikace, na směrovači ve funkci páteřního

směrovače, se paketům přidělila značka podle dané služby. Tato značka je tedy využita pro definování paketů, aby bylo možné pakety rozdělit do front. Protože se jedná pouze o jednu frontu, budou do této fronty zařazeny pakety všech služeb. Parametr *Queue Types* nastavuje typ fronty. Dále je frontě přidělena priorita, která zde ale nehraje žádnou roli, protože při spuštění služeb bude aktivní vždy pouze jeden ze systémů front. Při zadávání parametrů nemůže toto pole zůstat prázdné, proto byla priorita nastavena na hodnotu 1. Poslední dva parametry nastavují již zmíněnou minimální garantovanou přenosovou rychlost (*Limit At*) a maximální přenosovou rychlost (*Max Limit*). Při tomto nastavení se mezi jednotlivé služby rozdělí šířka pásma až 3 Mb/s.

The screenshot shows a configuration window for a queue type. On the left, under 'Name', 'FIFO' is selected. Below it, 'Parent' is set to 'global'. Under 'Packet Marks', three options are listed: 'VoIP', 'VLC', and 'FTP', each with a dropdown arrow and a double-headed arrow. On the right, 'Queue Type' is set to 'fifo'. 'Priority' is set to '1'. At the bottom, 'Limit At' is set to '2M' and 'Max Limit' is set to '3M', both with up/down arrows and the unit 'bits/s'.

Obr. 5.10: Nastavení fronty typu fifo.

Prioritní systém front (PQ)

Pro prioritní systém front byla nastavena hlavní fronta *PQ*, jak je zobrazeno na obr. 5.9. Tato fronta má, stejně jako fronta typu FIFO, nastaven parametr *Parent* na *global* a prioritu na hodnotu 1, viz obr. 5.10. Pod tuto frontu spadají další tři fronty. Už podle názvu je patrné, že každá fronta je určena pro jinou službu. Do fronty *PQ_VoIP* jsou zařazeny pakety hlasové služby. Do zbylých dvou front *PQ_VLC* a *PQ_FTP* jsou rozděleny pakety služeb streamovaného videa a přenosu dat. Aby bylo docíleno prioritního systému front na RouterBoardu, musela být maximální přenosová rychlost u všech front rovna maximální přenosové rychlosti hlavní fronty *PQ*. Minimální přenosová rychlost odpovídá rychlostem, při kterých nedochází k degradaci služby, ale pouze k omezení služby přenosu dat. Dále byla nastavena frontě *PQ_VoIP* priorita 1, frontě *PQ_VLC* priorita 2 a frontě *PQ_FTP* priorita 3.

Takže při obsluze tohoto systému front je nejprve vyzvána k odeslání dat fronta o prioritě 1. Pokud tato fronta obsahuje datový tok, který zabere celkovou šířku pásma hlavní fronty, z ostatních front se neodešlou žádná data. Pokud naopak fronta s prioritou 1 obsahuje datový tok s přenosovou rychlostí 1 Mb/s, je vybrána fronta

o prioritě 2. Opět rozhoduje, jaký datový tok fronta obsahuje. V případě, že obsahuje datový tok s přenosovou rychlostí 2 Mb/s, je společně s frontou o prioritě 1 využita celková šířka pásma hlavní fronty a z poslední fronty se neodešlou žádná data. Pokud však fronta o prioritě 2 obsahuje datový tok s rychlostí pouze 1,5 Mb/s, je z poslední fronty možné poslat data s přenosovou rychlostí 0,5 Mb/s.

V našem případě víme, že hlasová služba obsahuje datový tok s přenosovou rychlostí 320 kb/s a služba streamovaného videa obsahuje datový tok s přenosovou rychlostí 400 až 750 kb/s. Takže pro službu přenosu dat zbývá z celkové šířky pásma 1930 až 2280 kb/s.

Systém front se spravedlivou obsluhou (FQ)

V teoretické části (viz kap. 4) bylo vysvětleno, jaký dopad má různá velikost paketů služeb na spravedlivou obsluhu tohoto systému. Služba přenosu dat obsahuje pakety velikosti 1514 B, služba streamovaného videa 1370 B a hlasová služba 214 B. Takže služba přenosu dat nebo streamovaného videa může přesáhnout maximální povolenou rychlost a zabrat tak větší šířku pásma než služba hlasová. Systém FQ používá k odeslání dat algoritmus round-robin, který z každé fronty odešle vždy stejnou část dat. Proto byla pro všechny fronty, do kterých jsou rozděleny služby, nastavena stejná maximální přenosová rychlost na 800 kb/s. Při této rychlosti bude omezena pouze služba přenosu dat.

Fronty jsou pojmenovány podobně jako u prioritního systému, pouze obsahují v názvu *FQ*, jak je uvedeno na obr. 5.9. Opět byla nastavena hlavní fronta *FQ*, která má nastaven parametr *Parent* na *global* a prioritu na hodnotu 1, viz obr. 5.10. Pod tuto frontu spadají tři fronty, pro každou službu jiná. U těchto front byly nastaveny priority stejně jako u prioritního systému. Celková šířka pásma hlavní fronty je rovna součtu maximálních přenosových rychlostí front, které pod tuto frontu spadají.

Při obsluze systému je nejprve vyzvána k odeslání dat fronta *FQ_VoIP*, poté fronta *FQ_VLC* a nakonec fronta *FQ_FTP*. Přitom každá fronta může odeslat data s maximální přenosovou rychlostí 800 kb/s.

Systém front s váženou cyklickou obsluhou (WRR)

Systém WRR používá, stejně jako systém FQ, algoritmus round-robin. Tento systém však rozděluje jednotlivé fronty do tříd, kterým je přidělena určitá část celkové šířky pásma. Část šířky pásma je pak rozdělena spravedlivě mezi fronty dané třídy. Bohužel i zde není akceptována velikost paketů.

Nejprve byla vytvořena hlavní fronta *WRR*. Pod tuto frontu spadají dvě fronty, které jsou pojmenovány: *WRR_FIRST_CLASS* a *WRR_SECOND_CLASS*. Posloupnost front je uvedena na obr. 5.9. Hlavní fronta má nastaven parametr *Parent*

na *global* a prioritu na hodnotu 1 (viz obr. 5.10). Pro fronty *WRR_FIRST_CLASS* a *WRR_SECOND_CLASS* je priorita nastavena na hodnotu 1 a 2. Tyto fronty slouží jako třídy. Hlavní frontě byla nastavena maximální přenosová rychlost na hodnotu 3 Mb/s. Tato rychlost byla rozdělena mezi třídy podle určité váhy. Kde první třídě je přidělena váha 53,3 % a druhé třídě váha 46,7 %. Proto je první třídě přidělena část šířky pásma 1600 kb/s a druhé třídě část 1400 kb/s.

První třída obsahuje dvě fronty *WRR_VoIP* a *WRR_VLC*, které slouží pro rozdělení paketů hlasové služby a služby streamovaného videa. Frontě obsahující pakety hlasové služby je přidělena priorita 1 a frontě obsahující pakety služby streamovaného videa je přidělena priorita 2. Šířka pásma první třídy je rozdělena mezi fronty spravedlivě. Obě fronty mají tedy maximální přenosovou rychlost nastavenou na hodnotu 800 kb/s. Fronta pro službu přenosu dat spadá pod druhou třídu. Protože třída obsahuje pouze jednu frontu, je této frontě přiřazena celá šířka pásma a hodnota priority 1. Frontě *WRR_FTP* byla tedy nastavena maximální přenosová rychlost 1400 kb/s.

Při obsluze fronty je podle priority vyzvána nejprve první třída, ze které odešle data jako první fronta *WRR_VoIP* a poté fronta *WRR_VLC*. Protože systém *WRR* používá algoritmus round-robin, jsou data z obou front odeslána stejnou maximální přenosovou rychlostí 800 kb/s. Po obslužení první třídy je vyzvána k odeslání dat třída druhá, která obsahuje pouze jednu frontu, která má k dispozici šířku pásma 1400 kb/s.

Systém front s váženou spravedlivou obsluhou (WFQ)

Nastavení je stejné jako u systému *FQ*. Byly zde vytvořeny tři fronty, pro každou službu jiná. Fronty *WFQ_VoIP*, *WFQ_VLC* a *WFQ_FTP* jsou na obr. 5.9. Frontám byly nastaveny priority jako u prioritního systému. Všechny tři spadají pod hlavní frontu *WFQ*, u které je nastaveno *Parent* na *global* a priorita na hodnotu 1 (viz obr. 5.10).

Rozdíl oproti systému *FQ* je v přiřazování pásma jednotlivým frontám. Není zde pravidlem, že každá fronta odesílá data stejnou přenosovou rychlostí. Celková šířka pásma hlavní fronty je mezi jednotlivé služby rozdělena spravedlivě. Například u fronty *FQ_VoIP* je nastavena maximální přenosová rychlost na 800 kb/s. Přitom hlasová služba obsahuje datový tok o rychlosti 320 kb/s. Z původních 800 kb/s je tedy 480 kb/s nevyužito. U systému *WFQ* je pro frontu *WFQ_VoIP* nastavena maximální přenosová rychlost 400 kb/s. Takže bude nevyužito pouze 80 kb/s. Fronty hlasové služby a služby streamovaného videa zaberou dohromady 1200 kb/s z celkové šířky pásma, která je 3 Mb/s. Takže u fronty *WFQ_FTP*, tak mohla být nastavena rychlost až na 1800 kb/s. Šířka pásma je rozdělena efektivněji než u systému se

spravedlivou obsluhou FQ. Dalším rozdílem je použití typu fronty. U tohoto systému je použita fronta *bfifo*, která data odesílá po bajtech, takže pakety o větší velikosti nezaberou větší šířku pásma.

Systém založený na třídách s váženou spravedlivou obsluhou (CB WFQ)

Posloupnost front je stejná jako u systému WRR, kde byla nastavena hlavní fronta, pod kterou spadají dvě fronty. Tyto fronty slouží jako třídy. První třída obsahuje dvě fronty pro hlasovou službu (*CB-WFQ_VoIP*) a službu streamovaného videa (*CB-WFQ_VLC*), jak je zobrazeno na obr. 5.9. Fronta pro službu přenosu dat (*CB-WFQ_FTP*) spadá pod druhou třídu. Priority jsou také rozděleny stejným způsobem jako u systému WRR.

Rozdíl spočívá v rozdělení šířky pásma mezi jednotlivé fronty v třídách. Není zde použit algoritmus round-robin, kdy byla šířka pásma rozdělena mezi fronty stejným poměrem. Rozdělení šířky pásma je stejné jako u systému WFQ. První třída má přidělenou maximální přenosovou rychlost 1200 kb/s. Aby byla šířka pásma využita co nejlépe, byla frontě *CB-WFQ_VoIP* přidělena maximální přenosová rychlost pouze 400 kb/s, která je pro tuto službu dostačující. Frontě *CB-WFQ_VLC* pak byla přidělena zbylá část šířky pásma první třídy, tj. 800 kb/s. Pro druhou třídu a tedy i pro frontu *CB-WFQ_FTP* je možné využít přenosovou rychlost 1800 kb/s, která odpovídá zbývajícím částem z celkové šířky pásma hlavní fronty. Oproti systému front WRR je šířka pásma využita efektivněji. Obsluha fronty probíhá stejným postupem jako u systému front WRR.

5.4 Ověření konfigurace a zhodnocení výsledků

Po dokončení veškeré konfigurace byla provedena její kontrola a zhodnocení výsledků, které proběhlo na základě návodu k laboratorní úloze, viz příloha A. Cílem laboratorní úlohy je pochopit, z jakého důvodu se zavádí technologie QoS a její mechanismy, jaký systém front je vhodné použít vzhledem k poskytovaným službám a hlavně jakým způsobem nakonfigurovat aktivní síťové prvky, aby byla zajištěna kvalita služeb.

Podle návodu byla nejdříve doplněna požadovaná konfigurace na směrovačích. Dále došlo k ověření, s jakou přenosovou rychlostí služby komunikují při neomezeném provozu. Byly zjištěny následující rychlosti: služba přenosu dat 90 Mb/s a hlasová služba 320 kb/s. Rychlost pro službu streamovaného videa byla proměnlivá a pohybovala se mezi 400 až 750 kb/s. Před omezováním šířky pásma byly spuštěny všechny služby.

Omezení šířky pásma na 3 Mb/s

V dalším bodě bylo provedeno ověření funkce jednotlivých systémů front pro šířku pásma 3 Mb/s. Aby nedošlo k degradaci nebo k omezení některé služby, musela by šířka pásma být minimálně 92 Mb/s. Je tedy jasné, že musí dojít k omezení některé služby. Při rozdělení šířky pásma bylo podmínkou, aby nedošlo k degradaci hlasové služby a služby streamovaného videa. Byla tedy omezena služba přenosu dat. Rozdělení šířky pásma je na obr 5.9.

Při aktivní frontě typu FIFO byly všechny služby řazeny do jedné fronty. U hlasové služby docházelo ke zpoždění. Služba streamované videa probíhala bez ztráty obrazu či zvuku. Pro službu přenosu dat došlo k omezení šířky pásma.

Během sledování závislosti použitého systému front na kvalitě služeb, bylo také ověřeno, zdali všechny označované pakety byly klasifikovány a poté zařazeny do front. Jinými slovy, zda byla správně nastavena konfigurace a zdali nedocházelo ke ztrátě paketů. Podle obr. 5.11 bylo ověřeno že všechny vytvořené pakety jsou označovány a pakety, které nemají pole DSCP rovno 0, jsou zařazeny do příslušné fronty. Ověření proběhlo při aktivním prioritním systému front. Například pro službu přenosu dat bylo stanicí *PC1* zasláno 42 552 paketů. Na stanici *PC2* pak bylo klasifikováno a rozděleno do front také 42 552 paketů.

R1

#	Action	Chain	Src. Address	Packets
0	VoIP_PC1_klasifikace_znackovani			
0	✓ cha...	prerouting	172.27.141.6	45 728
1	VoIP_PC2_klasifikace_znackovani			
1	✓ cha...	prerouting	172.27.141.6	45 732
2	VoIP_klasifikace			
2	✗ mar...	forward		45 728
3	VLC_klasifikace_znackovani			
3	✓ cha...	prerouting	172.27.141.2	9 814
4	VLC_klasifikace			
4	✗ mar...	prerouting		9 217
5	FTP_klasifikace_znackovani			
5	✓ cha...	prerouting	172.27.141.2	42 552
6	FTP_klasifikace			
6	✗ mar...	prerouting		43 708

Name	Packets
... PQ	
📊 PQ	98 653
📊 PQ_FTP	43 708
📊 PQ_VLC	9 217
📊 PQ_Vo...	45 728

R2

#	Action	Chain	Src. Address	Packets
0	VoIP_klasifikace			
0	✗ mar...	prerouting		45 712
1	VLC_klasifikace_znackovani			
1	✓ cha...	prerouting	172.27.141.10	9 309
2	VLC_klasifikace			
2	✗ mar...	prerouting		9 732
3	FTP_klasifikace_znackovani			
3	✓ cha...	prerouting	172.27.141.10	43 708
4	FTP_klasifikace			
4	✗ mar...	prerouting		42 552

Name	Packets
... PQ	
📊 PQ	97 996
📊 PQ_FTP	42 552
📊 PQ_VLC	9 732
📊 PQ_Vo...	45 712

Obr. 5.11: Počet označovaných, klasifikovaných a zařazených paketů pro prioritní systém front.

Hlasová služba vyžaduje šířku pásma 320 kb/s, protože při komunikaci je použit kodek G.711, který přenáší data rychlostí 64kb/s. Celkem bylo navázáno pět relací, které dohromady tedy tvoří: $64 \cdot 5 = 320$ kb/s. U prioritního systému tedy došlo k rozdělení zbývající části celkové šířky pásma mezi služby streamovaného videa a přenosu dat. Jelikož je služba streamovaného videa zařazena do fronty s vyšší prioritou a vyžaduje šířku pásma 400 až 750 kb/s, byla službě přenosu dat poskytnuta šířka pásma 1930 až 2280 kb/s.

Také při použití ostatních systémů front docházelo pouze k omezování služby přenosu dat. U hlasové služby a služby streamovaného videa nedocházelo k žádné ztrátě či zpoždění paketů, protože šířka pásma pro tyto služby byla dostačující. Ale pokud dojde ke zmenšení celkové šířky pásma a bude mezi jednotlivé služby rozdělena nesprávně, dojde k degradaci služeb.

Omezení šířky pásma na 1,5 Mb/s

V dalším kroku byla šířka pásma omezena na 1,5 Mb/s. Rozdělení šířky pásma, konfigurací příslušných systémů front, mezi služby je na obr. 5.12. Přidělená část šířky pásma pro hlasovou službu a službu streamovaného videa je nedostačující, a protože obě služby používají nespolehlivý transportní protokol UDP, dojde k zahazování paketů. Pouze při aktivování prioritního systému nedošlo k degradaci těchto služeb, protože šířka pásma byla dostačující.

Name	Limit At (bits/s)	Max Limit (bits/s)	Name	Limit At (bits/s)	Max Limit (bits/s)
CB-WFQ		1500k	FQ		1500k
CB-WFQ_FIRST_CLASS		500k	FQ_FTP	400k	500k
CB-WFQ_VLC	200k	300k	FQ_VLC	400k	500k
CB-WFQ_VoIP	150k	200k	FQ_VoIP	400k	500k
CB-WFQ_SECOND_CLASS		1M	PQ		1500k
CB-WFQ_FTP	800k	1M	PQ_FTP	600k	1500k
FIFO	1M	1500k	PQ_VLC	600k	1500k
WRR		1500k	PQ_VoIP	300k	1500k
WRR_FIRST_CLASS		500k	WFQ		1500k
WRR_VLC	200k	250k	WFQ_FTP	800k	1M
WRR_VoIP	150k	250k	WFQ_VLC	200k	300k
WRR_SECOND_CLASS		1M	WFQ_VoIP	150k	200k
WRR_FTP	800k	1M			

Obr. 5.12: Rozdělení šířky pásma, konfigurací příslušných systémů front, mezi služby.

Opět byly postupně spuštěny služby a postupně aktivovány a deaktivovány jednotlivé systémy front. Pro všechny fronty docházelo k nekvalitnímu poskytování hlasové služby a služby streamovaného videa. Ztrátovost paketů způsobila výpadky obrazu a zvuku. Hlasový signál byl nesrozumitelný. Kolik paketů bylo u těchto služeb zahazeno je znázorněno na obr. 5.13, pro systém front s váženou cyklickou

obsluhou WRR. Pro službu streamovaného videa bylo na směrovači *R1* klasifikováno 12 749 paketů. Z fronty pro tuto službu (*WWR_VLC*) však bylo odesláno pouze 5 441 paketů. Celkem 7 308 paketů bylo zahozeno. Jedná se o ztrátu 53 % všech dat. V reálné datové síti, kde je například poskytována služba internetové televize, je výše této ztráty nepřijatelná. U hlasové služby došlo ke ztrátě 12 118 paketů z celkem klasifikovaných 54 009 paketů. Ztráta je rovna 22,5 %. V teoretické části (viz kap. 1.2) bylo uvedeno, že pokud je ztrátovost větší jak 10 %, bude kvalita hovoru velice nízká a slyšitelnost minimální.

R1					R2				
#	Action	Chain	Src. Address	Packets	#	Action	Chain	Src. Address	Packets
::: VoIP_klasifikace_znackovani					::: VoIP_klasifikace				
0	✓ cha...	prerouting	172.27.141.6	54 009	0	✗ mar...	prerouting		54 009
::: VoIP_PC2_klasifikace_znackovani					::: VLC_klasifikace_znackovani				
1	✓ cha...	prerouting	172.27.141.6	54 006	1	✓ cha...	prerouting	172.27.141.10	12 749
::: VoIP_klasifikace					::: VLC_klasifikace				
2	✗ mar...	forward		54 009	2	✗ mar...	prerouting		13 457
::: VLC_klasifikace_znackovani									
3	✓ cha...	prerouting	172.27.141.2	13 456					
::: VLC_klasifikace									
4	✗ mar...	prerouting		12 749					
WRR global					WRR global				
				78 601					79 144
WRR_... WRR				47 529	WRR_... WRR				47 843
W... WRR_FIRST... VLC				5 441	W... WRR_FIRST... VLC				5 482
W... WRR_FIRST... VoIP				41 891	W... WRR_FIRST... VoIP				42 162

Obr. 5.13: Počet označovaných, klasifikovaných a zařazených paketů pro systém front s váženou cyklickou obsluhou.

Jakým způsobem tedy rozdělit šířku pásma mezi služby, aby nedocházelo ke ztrátě paketů a nebyla tak pozorovatelná degradace hlasové služby a služby streamovaného videa? Ze znalosti minimální šířky pásma je nutné pro hlasovou službu vyčlenit v každém systému front minimálně 320 kb/s a službě streamovaného videa pak alespoň 750 kb/s. Potom službě přenosu dat je možné přidělit zbývajících 430 kb/s. Tak bude zajištěno, že ztrátovost paketů pro hlasovou službu a službu streamovaného videa bude téměř 0 % a službě přenosu dat bude přidělena maximální možná šířka pásma.

Zhodnocení výsledků

V měření se podařilo rozdělit šířku pásma 3 Mb/s spravedlivě mezi služby. Pro šířku pásma 1,5 Mb/s bylo dosaženo degradace služeb pracujících v reálném čase a tím tak bylo znázorněno, jak důležité je rozdělení šířky pásma mezi jednotlivé služby. Na základě měření můžeme také usoudit, že parametry QoS, jako je šířka pásma a ztrátovost paketů, jsou na sobě závislé. Pokud u služeb závislých na čase

je nastavena nedostačující šířka pásma a je používán transportní protokol UDP, dojde k zahazování paketů. Při měření s celkovou šířkou pásma 1,5 Mb/s došlo k omezení šířky pásma pro hlasovou službu z požadovaných 320 kb/s na 250 kb/s. Omezením šířky pásma o 70 kb/s tak došlo ke ztrátě 22,5%. Stejně tak pro službu streamovaného videa došlo k omezení šířky pásma z požadovaných 750 kb/s na 250 kb/s. Toto omezení šířky pásma mělo za následek 53 % zahozených paketů.

Nastavením šířky pásma je tedy možné služby omezit a tím tak ostatní zvýhodnit. Jak nastavit šířku pásma je také závislé na použitém systému front. Pokud například bude použit prioritní systém front, je na základě jeho funkce nutné nastavit všem službám stejnou šířku pásma, která odpovídá celkové šířce pásma. Tento systém front vyhovuje, pokud chceme preferovat nějakou službu před ostatními službami. Pokud požadujeme, aby se všemi službami bylo zacházeno stejným způsobem, použijeme systém front se spravedlivou obsluhou, kde je nutné brát ohled také na velikost paketů jednotlivých služeb.

Systém front s váženou cyklickou obsluhou je pak možné použít v síti, kde je například požadavek na zvýhodnění určité skupiny služeb před ostatními, ale s podmínkou, že se všemi službami v této skupině bude zacházeno stejným způsobem. Nebo také naopak, kdy chceme určitou skupinu služeb znevýhodnit. Například v nějaké podnikové síti, kde je požadováno omezení služby streamovaného videa a přenosu objemných dat. Jestliže nechceme zvýhodnit nebo znevýhodnit skupinu služeb, ale pouze jednotlivé služby, je možné použít systém front s váženou spravedlivou obsluhou. Možné je však také použití systému založeného na třídách s váženou spravedlivou obsluhou. Tento systém je vhodné použít v síti, ve které chceme zvýhodnit určitou skupinu služeb, ale nechceme, aby s jednotlivými službami v této skupině bylo zacházeno stejným způsobem. Jedná se tedy o spojení dvou předchozích systémů.

6 ZÁVĚR

V práci se zabývám technologií Quality of Services, pomocí které je možné zajistit kvalitu poskytovaných služeb. První část práce je zaměřena na teoretický rozbor této technologie. Nejdříve jsem popsal služby, které jsou v dnešních datových sítích poskytovány, a jejich závislost na parametrech QoS. Technologie QoS je poskytována mechanismy IntServ a DiffServ. V další části teorie jsou tedy vysvětleny tyto mechanismy a jejich procesy, kde nejdůležitější jsou procesy mechanismu DiffServ, mezi které patří klasifikace paketů, značkování paketů a správa front. Tyto procesy jsou rozděleny mezi aktivní prvky sítě, které pak dohromady tvoří DiffServ doménu. V posledním bodě jsem se zaměřil na důkladný popis jednotlivých systémů front.

V druhé části práce se zabývám návrhem laboratorní úlohy, kde je cílem ověření teoretických znalostí. Při návrhu bylo důležité, aby topologie obsahovala co nejmenší počet směrovačů. Jako směrovače byly použity RouterBoardy 493G. Komunikace probíhá mezi dvěma stanicemi. Pro kompletní DiffServ doménu je nutné použít minimálně tři směrovače. Ale po důkladné analýze možné konfigurace RouterBoardů jsem došel k závěru, že je možné použít pouze dva směrovače. Sít laboratorní úlohy tedy byla navržena pro dvě stanice propojené přes dva směrovače. V síti byl také použit VoIP server, který zajišťoval hlasovou službu. Dále byly použity služby přenosu dat a streamovaného videa.

Poslední část práce je zaměřena na samotné testování konfigurace a ověření teoretických poznatků. V příloze A je obsažen návod, podle kterého je testování konfigurace možné provést. V prvním bodě jsem zjistil, jakou přenosovou rychlostí služby komunikují, pokud nejsou omezeny. Na základě zjištěných rychlostí jsem šířku pásma omezil na 3 Mb/s. Šířku pásma jsem mezi jednotlivé služby rozdělil poměrem, při kterém byla omezena pouze služba přenosu dat. Ověřil jsem, že značkování a klasifikace je nakonfigurovaná správně, a proto jsem postupně aktivoval a deaktivoval jednotlivé systémy front a pozoroval jsem, jakým způsobem ovlivňují kvalitu služeb. Hlasová služba a služba streamovaného videa probíhaly bez jakékoliv degradace. Aby bylo možné ukázat, jaký vliv má na kvalitu služeb špatné rozdělení šířky pásma, omezil jsem šířku pásma na 1,5 Mb/s a rozdělil ji mezi služby tak, aby docházelo k degradaci hlasové služby a služby streamovaného videa. Následným měřením jsem tuto skutečnost ověřil a šířku pásma jsem poté rozdělil poměrem, při kterém k degradaci služeb nedocházelo. Na závěr se zabývám vhodným použitím systému front na základě poskytovaných služeb.

LITERATURA

- [1] ČÍKA, P. *Multimediální služby*. Brno: Vysoké učení technické v Brně, 2012. s. 1-127. ISBN: 978-80-214-4443- 0.
- [2] KOTON, J. *Moderní síťové technologie*. Brno: Vysoké učení technické v Brně, 2014. s. 1-191. ISBN: 978-80-214-5026- 4.
- [3] WALLACE, K. *Cisco VoIP*. Computer Press, a.s., 2009. ISBN 978-80-251-2228-0.
- [4] *Požadavky různých druhů provozu na kvalitu služby*. Brno: Vysoké učení technické v Brně, 2014.
- [5] BRADEN, R., CLARK, D., SHENKER, S. *Integrated Services in the Internet Architecture*. RFC 1633, červen 1994. Dostupné z URL: <<https://tools.ietf.org/html/rfc1633>>.
- [6] TOS: Abbreviation for Type of Service. *INACON Protocol Help* [online]. 2010 [cit. 2014-12-16]. Dostupné z URL: <http://www.inacon.de/ph/data/IPv4/Header_fields/IP-Header-Field-TOS_OS_RFC-791.htm>.
- [7] ALMQUIST, P. *Type of Service in the Internet Protocol Suite*. RFC 1349, červenec 1992. Dostupné z URL: <<https://tools.ietf.org/html/rfc1349>>.
- [8] NICHOLS, K., BLAKE, S., BAKER, F., BLACK, D. *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*. RFC 2474, prosinec 1998. Dostupné z URL: <<https://tools.ietf.org/html/rfc2474>>.
- [9] BRADEN, R., ZHANG, L., BERSON, S., HERZOG, S., JAMIN, S., *Resource ReSerVation Protocol (RSVP)*. RFC 2205, srpen 1997. Dostupné z URL: <<https://tools.ietf.org/html/rfc2205>>.
- [10] HON, P. Jak funguje řízení datových toků s QoS. *Connect* [online]. 2012 [cit. 2014-12-13]. Dostupné z URL: <<http://connect.zive.cz/clanky/jak-funguje-rizeni-datovych-toku-s-qos/sc-320-a-161738>>.
- [11] BLAKE, S., BLACK, D., CARLSON, M., DAVIES, E., WANG Z., WEISS W. *An Architecture for Differentiated Services*. RFC 2475, prosinec 1998. Dostupné z URL: <<http://www.hjp.at/doc/rfc/rfc2475.txt>>.
- [12] GROSSMAN, D. *New Terminology and Clarifications for Diffserv*. RFC 3260, duben 2002. Dostupné z URL: <<https://tools.ietf.org/html/rfc3260>>.

- [13] DSCP: Abbreviation for Differentiated Services Code Point. *INACON Protocol Help*. [online]. 2010 [cit. 2014-12-16]. Dostupné z URL: <http://www.inacon.de/ph/data/IPv4/Header_fields/index.php>.
- [14] Implementing Quality of Service Policies with DSCP. *Cisco* [online]. 2008 [cit. 2014-11-28]. Dostupné z URL: <<http://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html>>.
- [15] HEINANEN, J., BAKER, F., WEISS, W., WROCLAWSKI, J. *Assured Forwarding PHB Group*. RFC 2597, červen 1999. Dostupné z URL: <<https://tools.ietf.org/html/rfc2597>>.
- [16] JACOBSON, V., NICHOLS K., PODURI, K. *An Expedited Forwarding PHB*. RFC 2598, červen 1999. Dostupné z URL: <<https://tools.ietf.org/html/rfc2598>>.
- [17] DAVIE, B., CHARNY, A., BENNETT, J.C.R., BENSON, K., LE BOUDEC J.Y., COURTNEY, W., DAVARI, S., FIROIU, V., STILIADIS, D. *An Expedited Forwarding PHB (Per-Hop Behavior)*. RFC 3264, březen 2002. Dostupné z URL: <<https://tools.ietf.org/html/rfc3246>>.
- [18] *Zajištění kvalitativní podpory služeb v podnikových sítích*. Brno: Vysoké učení technické v Brně, 2014.
- [19] ODOM, W., HEALY R., MEHTA N. *Směrování a přepínání sítí*. Computer Press, a.s., 2009. ISBN 978-80-251-2520-5.
- [20] MEDHI, D., RAMASAMY, K. *Network Routing: Algorithms, Protocols, and Architectures*. Morgan Kaufmann, 2007. ISBN 978-0-12-088588-6.
- [21] BOUŠEK, P. Cisco QoS 4 – garance rychlosti – řazení do front – Queuing: Congestion Management – Queuing. *Samuraj-cz* [online]. 2009 [cit. 2015-05-18]. Dostupné z URL: <<http://www.samuraj-cz.com/clanek/cisco-qos-4-garance-rychlosti-razeni-do-front-queuing/>>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

AF	Assured Forwarding
BA	Behaviour Aggregate
BE	Best-Effort
CBQ	Class-Based Queueing
CB WFQ	Classed-Based Weighted Fair Queueing
CS	Class Selector
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DS	DiffServ Differentiated Services
DSCP	Differentiated Services Code Point
ECN	Explicit Congestion Notification
EF	Expedited Forwarding
FIFO	First In First Out
FQ	Fair Queueing
FTP	File Transfer Protocol
IntServ	Integrated Services
IP	Internet Protocol
IPv4	Internet Protocol version 4
MF	Multi-Field Classification
PHB	Per-Hop Behavior
PQ	Priority Queueing
QoS	Quality of Services
RTP	Real-Time Transport Protocol
RSVP	Resource Reservation Protocol

SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
ToS	Type of Services
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol
WFQ	Weighted Fair Queueing
WRR	Weighted Round Robin

SEZNAM PŘÍLOH

A	Návod k laboratorní úloze	67
A.1	Teoretický úvod	67
A.2	Pokyny k vypracování	71
A.2.1	Topologie a importování konfigurace	71
A.2.2	Doplnění konfigurace	72
A.2.3	Ověření nastavené konfigurace	75
B	Obsah přiloženého CD	77

A NÁVOD K LABORATORNÍ ÚLOZE

A.1 Teoretický úvod

Pro efektivní zajištění kvality služeb je nezbytná znalost datového provozu, který se v rámci současných datových a komunikačních sítí skládá z mnoha služeb. Základní dělení služeb se provádí podle jejich závislosti na čase. Každá služba je závislá na parametrech QoS (Quality of Services), mezi které patří ztrátovost, zpoždění, kolísání zpoždění a šířka pásma. Pro služby závislé na čase je důležité, aby byly přeneseny s minimálním zpožděním, kdy určitá míra ztrátovosti je tolerována. Mezi takové služby patří například přenos hlasu nebo videa. Druhou skupinou jsou pak služby, kde jejich přenos není závislý na čase. Tedy služby, u kterých není kvalita citlivá na zpoždění, ale klade velký důraz na nulovou ztrátovost. Jedná se například o přenos dat. Základní rozdělení služeb je uvedeno v tab. A.1.

Mechanismus Diferencovaných služeb (DiffServ)

DiffServ dělí služby v síti podle jejich požadavků na přenos. Každá služba je přiřazena do určité třídy. Směrovače pak s každou třídou zacházejí odlišně. Odlišného zacházení pro jednotlivé třídy je dosaženo pomocí řízeného přidělování síťových zdrojů. Mechanismus DiffServ (Differentiated Services) provádí procesy značkování paketů, klasifikace paketů a rozdělování paketů do front.

Existuje také mechanismus Integrovaných služeb (IntServ), který po celé trase rezervuje pásmo a požadované zpoždění. Nevýhodou tohoto mechanismu je velká režie před zahájením spojení. Výchozím nastavením všech síťových prvků je zacházení Best-Effort, kdy je s pakety různých služeb zacházeno stejným způsobem.

Značkování paketů

Dříve se provádělo značkování pomocí změny hodnoty pole ToS (Type of Services), které je v hlavičce IP datagramu. Pole ToS udává význam o absolutní prioritě daného paketu. Skládá se z osmi bitů, kde první tři bity určují danou prioritu, tzv. IP Precedence. V mechanismu DiffServ se pole ToS označuje DS, podle anglického názvu Differentiated Services. Rozděluje se na dvě další pole. První pole je označováno DSCP (Differentiated Services Code Point) a zahrnuje prvních šest bitů, které nejsou kódové označení diferencované služby a jsou používány k označení třídy. Zbýlé dva bity spadají pod pole ECN (Explicit Congestion Notification). V mechanismu DiffServ proces značkování neudává význam o absolutní prioritě paketu, ale určuje identifikátor třídy. Pro identifikaci třídy se nastavuje hodnota pole DSCP, které se v protokolu IPv4 (Internet Protocol version 4) nachází v hlavičce IP datagramu.

Kvůli kompatibilitě s polem ToS a jeho částí IP Precedence je zavedeno osm tříd, které jsou označeny zkratkou CS0 až CS7 (Class Selector – CS). Jednotlivé třídy se rozlišují na základě hodnoty prvních tří bitů. Obecně platí, že do třídy s větší hodnotou se přiřazují služby, které kladou větší požadavky na přenos. Dále byl zaveden způsob zacházení s pakety dané služby, tzv. Per-Hop Behavior – PHB. Dochází k rozdělení třídy CS1 až CS5 na další podtřídy, viz tab. A.1. Jsou specifikovány tři základní způsoby zacházení:

- Best-Effort – BE: standardní PHB dostane nejnižší prioritu,
- Assured Forwarding – AF: pro služby, které kladou důraz na spolehlivost,
- Expedited Forwarding – EF: pro služby, které kladou důraz na zpoždění a kolísání zpoždění při nízké ztrátovosti.

Klasifikace paketů

Pakety, které nejsou označovány, projdou procesem klasifikace a následně jsou označovány. Pokud jsou příchozí pakety již označovány, projdou procesem klasifikace, který je na základě značky rozdělí do front. V mechanismu DiffServ je značkou hodnota pole DSCP.

Systémy front

Jedním ze způsobů zajištění kvality služeb na směrovačích je proces řazení paketů do oddělených front. Existuje sedm základních systému front:

- systém fronty typu FIFO (First In First Out),
- prioritní systém front (Priority Queuing – PQ),
- systém front se spravedlivou obsluhou (Fair Queueing – FQ),
- systém front s váženou cyklickou obsluhou (Weighted Round Robin – WRR),
- systém front s váženou spravedlivou obsluhou (Weighted Fair Queueing – WFQ),
- systém založený na třídách s váženou spravedlivou obsluhou (Class-Based Weighted Fair Queueing – CB WFQ),
- systém založený na třídách s prioritní frontou (Low Latency Queuing – LLQ).

Fronta typu FIFO je výchozí systém front každého směrovače. Jedná se o jedinou frontu, takže zde není žádný prioritní mechanismus. Pakety jsou do fronty řazeny v pořadí, v jakém byly přijaty (First In) a ve stejném pořadí jsou také odeslány (First Out).

Prioritní systém front obsahuje více front, kde každá fronta má určitou prioritu. Přicházející pakety jsou klasifikovány a následně, podle toho do jaké třídy patří, přiřazeny do fronty o dané prioritě. Pakety ve frontě s největší prioritou jsou upřednostněny před pakety ve frontách s nižší prioritou.

Systém FQ řadí přijaté pakety do M front. Pro odesílání paketů používá algoritmus round-robin, který během každého cyklu vybere k odeslání maximálně jeden paket z každé fronty. Vzhledem k různé velikosti paketů dochází k různému obsazení šířky pásma. Pakety o větší velikosti zaberou větší šířku pásma, i když patří do fronty s nejnižší prioritou.

Systém WRR je schopen pro jednotlivé třídy zajistit požadovanou šířku pásma. Pakety jsou rozděleny do n tříd. Dále jsou pakety v rámci každé třídy rozděleny do m front. Ke každé třídě je přiřazena váhová hodnota V_n , která vyjadřuje procentuální využití šířky pásma. Pro předání paketů na výstup se používá dvouúrovňové cyklické plánování round-robin.

Systém WFQ, podobně jako u systému WRR, jednotlivým frontám přidá váhovou hodnotu, určující procentuální využití šířky pásma. Rozdělení front je stejné jako u systému FQ. V případě systému FQ byl paket odeslán bez ohledu na jeho velikost. Systém WFQ problém s různou velikostí jednotlivých paketů vyřešil pomocí teoretického modelu cyklické obsluhy. V teoretickém modelu si můžeme představit, že jsou pakety na výstup posílány v určitých blocích, např. bit po bitu. Před odesláním paketů musí dojít k jejich složení. Pakety s větší velikostí se budou skládat déle, proto tedy i jejich odeslání na výstup bude trvat déle.

V systému CB WFQ dochází ke kombinaci systému WRR a WFQ. Pakety jsou podobně jako u systému WRR rozděleny do n tříd. Poté jsou v každé třídě rozděleny do odpovídající fronty. Každé třídě je přidělena váha vyjadřující procentuální vyhrazení šířky pásma. Hlavní změna oproti systému WRR je v používání obsluhy front. Systém CB WFQ používá pro obsluhu front stejný postup jako systém WFQ.

Posledním systémem front je LLQ. Tento systém má rozdělení a obsluhu front stejnou jako systém CB WFQ. Výhodou tohoto systému je vytvoření prioritní fronty na úrovni tříd. Této frontě je přidělena určitá část šířky pásma a je upřednostněna před ostatními frontami.

DiffServ doména

Aby nedocházelo k vytížení aktivních síťových prvků, jsou procesy mechanismu DiffServ rozděleny mezi směrovače v síti. DiffServ doména se skládá z hraničních a páteřních směrovačů. Na hraničním směrovači se provádí proces klasifikace a značkování. Pakety všech služeb musejí být nejdříve označovány, proto jsou na hraniční směrovače připojena koncová zařízení.

Hraniční směrovače jsou propojeny pomocí páteřních směrovačů, které jsou více zatížené směrováním. Proto jsou na těchto směrovačích prováděny procesy klasifikace a řazení paketů do front. Může se zdát, že řazení do front patří mezi náročné procesy mechanismu DiffServ, ale správa front je nedílnou součástí každého směrovače.

Tab. A.1: Rozdělení tříd podle hodnoty pole DSCP v závislosti na PHB.

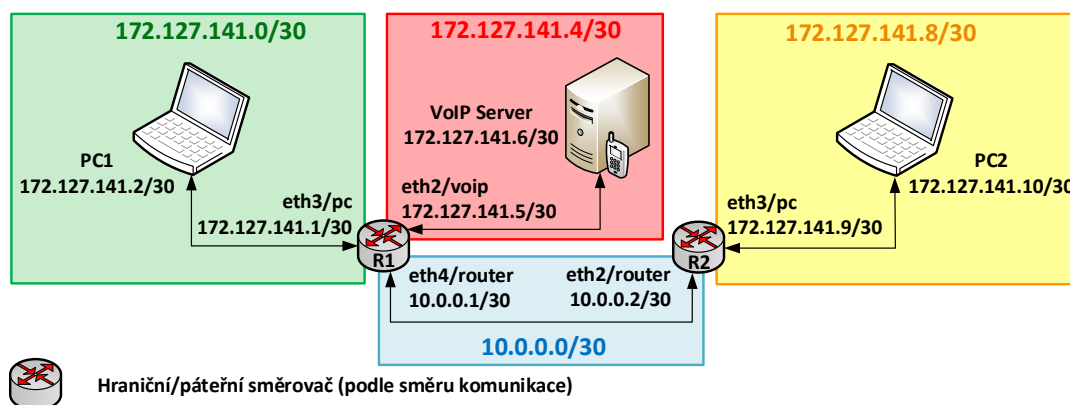
Třída	Značení třídy	IP Precedence	DSCP	Hodnota	Služby
CS7	CS7	7	111 000	56	směrovací protokoly v lokální síti
CS6	CS6	6	110 000	48	směrovací protokoly
CS5	EF	5	101 110	46	hlasové služby
	CS5		101 000	40	
CS4	AF43	4	100 110	38	videokonference
	AF42		100 100	36	
	AF41		100 010	34	
	CS4		100 000	32	
CS3	AF33	3	011 110	30	uživatelsky kritické služby
	AF32		011 100	28	
	AF31		011 010	26	
	CS3		011 000	24	
CS2	AF23	2	010 110	22	transakční a interaktivní služby
	AF22		010 100	20	
	AF21		010 010	18	
	CS2		010 000	16	
CS1	AF13	1	001 110	14	objemná data
	AF12		001 100	12	
	AF11		001 010	10	
	CS1		001 000	8	
CS0	BE	0	000 000	0	data nevyžadující vysokou prioritu Best-Effort

A.2 Pokyny k vypracování

A.2.1 Topologie a importování konfigurace

Topologie je znázorněna na obr. A.1. Na *PC1* i *PC2* zapněte aplikaci winbox. Z *PC1* se připojte ke směrovači *R1* a z *PC2* ke směrovači *R2*. Po úspěšném připojení klikněte na položku *Files*. Do nově otevřeného okna zkopírujte soubor *R1/R2_3000kb.rsc* ze složky *D:\BP_DiffServ\RB_zaloha*. Dále po kliknutí na *New Terminal* importujte nahrané soubory, tj. na směrovači *R1* soubor *R1_3000kb.rsc* a na směrovači *R2* soubor *R2_3000kb.rsc*. Import lze provést zadáním příkazu `import file="soubor"`. **Po importování souborů si důkladně projděte jednotlivá nastavení na směrovači. Znalost topologie a konfigurace je v dalších krocích nezbytná.**

Soubor *R1_3000kb.rsc* obsahuje konfiguraci směrovače *R1*. Názvy rozhraní směrovače, které je možné zobrazit otevřením nabídky *Interface*, byly změněny podle připojeného zařízení. IP Adresy, pro jednotlivá rozhraní, byly nastaveny v položce *IP/Address*. Pro přiřazení adresy stanici *PC1* byl nastaven DHCP server. Jeho konfiguraci naleznete v *IP/DHCP Server*. *VoIP* server obsahuje statickou IP adresu, proto na rozhraní *voip* nebyl nastaven DHCP server. Aby byla možná komunikace mezi sítěmi, musela být přidána cesta do *IP/Routes*. Kde *Dst. Address* určuje síť, ve které se nachází cílová stanice a *Gateway* určuje IP adresu rozhraní, na které budou pakety přeposlány. Soubor *R2_3000kb.rsc* obsahuje podobná nastavení s rozdílem v IP adresách a směrování.



Obr. A.1: Topologie laboratorní úlohy.

A.2.2 Doplnění konfigurace


Nastavení klasifikace a značkování paketů na směrovači R1


Na stanici *PC1* i *PC2* byly nainstalovány aplikace, které poskytují služby přenosu dat, streamovaného videa a hlasovou službu. Pro přenos dat byla zvolena aplikace *FilleZilla client* a *FilleZilla server*, pro streamované video aplikace *VLC* a pro hlasovou službu aplikace *MicroSIP*.

Otevřete okno, které obsahuje pravidla pro klasifikaci a značkování, kliknutím na nabídku *IP/Firewall*, kde dále zvolte záložku *Mangle*. Po otevření se zobrazí předpřipravené pravidla pro hlasovou službu a službu přenosu dat. Zobrazte si pravidlo *VoIP_PC1_klasifikace_znackovani*. Každé pravidlo obsahuje záložky *General*, *Advance* a *Extra*, pomoci kterých je možné nastavit proces klasifikace. Pakety hlasové služby, které jsou určeny pro stanici *PC1*, jsou klasifikovány na základě IP adres, transportního protokolu UDP (User Datagram Protocol) a rozhraní, na kterém jsou přijaty. Tyto parametry jsou obsaženy v záložce *General*. Protože je *VoIP server* nastaven jako proxy server, jsou všechny pakety odeslané serverem označovány na rozhraní *voip*. Parametr *Chain: prerouting* uvádí, že se pravidlo provede na vstupním rozhraní, na kterém byl paket přijat. V RouterOS se mohou procesy provádět postupně v *preroutingu*, *forwardu* a *postroutingu*. V poslední záložce *Action* se nastavuje značkování paketů, kde byla vybrána možnost *change DSCP (TOS)* a nastavena změna pole DSCP na hodnotu 46, podle tab. A.1. Podobné nastavení bylo provedeno i pro odchozí pakety z *VoIP serveru*, směrované stanici *PC2*.

Dále si zobrazte pravidlo *VoIP_klasifikace*, pro které byly v záložce *General* nastaveny parametry: *Chain: forward* a *In. Interface: voip*. V záložce *Advance* pak byl nastaven parametr *DSCP (TOS): 46*. Pro tyto pakety byla v záložce *Action* vybrána možnost *mark packet*. Pomocí této možnosti byla paketům přidělena značka *VoIP*, která slouží pro rozdělení do front. Pro klasifikaci příchozích paketů byl zvolen *Chain: forward* z důvodu, aby se pakety nejdříve označovaly (*prerouting*) a poté klasifikovaly na základě značky.

Prohlédněte si také pravidlo *FTP_klasifikace_znackovani*. Pakety jsou klasifikovány a značkovány na rozhraní *pc*, protože všechny datový provoz služby přenosu dat, který je vytvořen na stanici *PC1*, musí být označován. U pravidla *FTP_klasifikace* si uvědomte, z jakého důvodu je klasifikace prováděna na rozhraní *router*.

Pro službu streamovaného videa nastavte podobným postupem pravidla klasifikace a značkování odchozích paketů a klasifikace příchozích paketů. Nové pravidlo přidáte kliknutím na . Služba streamovaného videa používá protokol UDP a Dst. Port 5004, nezapomeňte také na IP adresy. Hodnotu pole DSCP nastavte podle tab. A.1. **U klasifikace příchozích paketů nastavte v záložce Action, pro možnost mark packet, značku VLC. Je to důležité v rámci správné**


funkce jednotlivých systémů front. Položku Passthrough odškrtněte. Tím nastavíte, že pokud paket vyhovuje parametrům daného pravidla, dalšími pravidly již neprochází. Pravidla si pojmenujte podobně jako u předem vytvořených pravidel, kliknutím na . Vytvořená pravidla přesuňte pod pravidlo *VoIP_klasifikace*.

Nastavení klasifikace a značkování paketů na směrovači R2

Na směrovači *R2* jsou v záložce *Mangle* předpřipravené pravidla pro hlasovou službu a službu přenosu dat, jako tomu bylo na směrovači *R1*. Prohlédněte si nastavení jednotlivých pravidel pro službu přenosu dat. Nastavení je stejné jako na směrovači *R1*, pouze IP adresy jsou opačné. Pro hlasovou službu je nastaven pouze proces klasifikace příchozích paketů. Odchozí pakety ze stanice *PC2* není nutné značkovat, protože jsou přeposlány přes *VoIP server*. Potřeba je tedy značkovat až pakety odeslané *VoIP serverem*, jak jste nastavili na směrovači *R1*. Na směrovači *R2* se provádí klasifikace na rozhraní *router*.

Podobně, jako pro směrovač *R1*, nastavte zbývající pravidla pro službu streamovaného videa. Pravidla budou téměř stejná, změna bude pouze v IP adresách. **Nezapomeňte při nastavení klasifikace příchozích paketů nastavit v záložce *Action* značku *VLC*.** Vytvořená pravidla přesuňte pod pravidlo *VoIP_klasifikace*.

Nastavení systémů front

Nastavení provádějte na směrovači *R1*. V položce *Queues* vyberte záložku *Queues Tree*. Po otevření se vám zobrazí jednotlivé systémy front. Celková šířka pásma, u všech systémů front kromě *FQ*, byla zvolena 3 Mb/s. Jejich konfigurace není kompletní. Pro přidání nové fronty klikněte na . Zobrazené parametry mají následující význam:

- Name: název fronty,
- Parent: nadřazená fronta,
- Packet Marks: určuje, jaké pakety budou do této fronty zařazeny,
- Queue Typ: typ fronty,
- Priority: udává prioritu 1 až 8, kde 1 je nejvyšší priorita a 8 nejnižší priorita,
- Limit At: minimální garantovaná rychlost,
- Max Limit: maximální rychlost,

Pro frontu typu *FIFO* byla vytvořena fronta s názvem *FIFO*, která má nastavený parametr *Parent* na *global* a prioritu na hodnotu 1. Možnost *global* určuje, že se řazení do front provede v *postrouting*. Pro všechny fronty, kromě systému *WFQ* a *CB WFQ*, byla nastavena fronta typu *pfifo*, která data odesílá po paketech. *Max limit* je nastaven na šířku pásma 3 Mb/s a minimální garantovaná rychlost na hodnotu 2 Mb/s.

U systému PQ je nutné doplnit frontu pro hlasovou službu. Vytvořte tedy novou frontu, kde nastavte tyto parametry: *Name: PQ_VoIP*, *Parent: PQ*, *Packet Marks: VoIP*, *Queue Type: pfifo*, *Priority: 1*, *Limit At: 300 kb/s* a *Max Limit: 3 Mb/s*. Tím docílíte, že při obsluze tohoto systému front bude jako první vyzvána k odeslání dat fronta pro hlasovou službu. Pokud obsahuje datový tok o rychlosti 3 Mb/s, data z ostatních front se neodešlou. Pokud zabere pouze část z celkové šířky pásma, je zbytek šířky pásma rozdělen mezi fronty *PQ_VLC* a *PQ_FTP*.

Stejným postupem doplňte frontu pro hlasovou službu také u systému FQ. Opět vytvořte novou frontu, kde parametry nastavte jako u ostatních front tohoto systému s výjimkou priority, kterou nastavte na hodnotu 1. Při obsluze této fronty odešlou všechny fronty data rychlostí 800 kb/s. Rychlost může být ale odlišná, záleží na velikostech jednotlivých paketů. Fronty jsou vyzvány k odeslání dat v pořadí podle priority.

Pro systém WRR je nutné doplnit druhou třídu, která bude obsahovat frontu pro pakety služby přenosu dat. Proto vytvořte novou frontu, která bude mít stejný parametr *Parent* jako fronta *WRR_FIRST_CLASS*. Vhodně třídu pojmenujte. Prioritu nastavte na hodnotu 2 a *Max limit* na hodnotu 1400 kb/s, která odpovídá zbývajícím částem šířky pásma hlavní fronty *WRR*. *Limit At* nastavte na 1100 kb/s. Dále přidejte další frontu *WRR_FTP*, u které nastavte *Parent* na název, který jste zvolili při vytvoření druhé třídy. Hodnoty *Limit At* a *Max limit* nastavte na 1100 kb/s a 1400 kb/s. Nezapomeňte vybrat parametrem *Packet mark* službu přenosu dat (*FTP*). Při obsluze systému dojde k odeslání dat nejdříve z fronty *WRR_VoIP*, poté z fronty *WRR_VLC* a nakonec z fronty, kterou jste vytvořili pro službu přenosu dat.

Systém front WFQ je nastaven stejně jako systém FQ, s rozdílem v přidělení různé šířky pásma pro jednotlivé fronty. Doplňte opět systém o frontu, do které se budou zařazovat pakety hlasové služby. Parametry nastavte stejně jako u systému FQ, ale *Limit At* a *Max Limit* nastavte na hodnotu 300 kb/s a 400 kb/s. Typ fronty zvolte *bfifo*, která data odesílá po bajtech. Výhoda tohoto systému je v efektivnějším rozdělení šířky pásma mezi jednotlivé služby.

Posledním systémem je CB WFQ. Systém má stejnou posloupnost front jako systém WRR, ale obsluha a rozdělení šířky pásma pro jednotlivé fronty je stejná jako u systému WFQ. Doplňte tedy systém o frontu, pro hlasovou službu, kde nastavte všechny parametry jako u fronty *WRR_VoIP*, ale typ fronty zvolte *bfifo*, jako u WFQ. Hodnotu *Max limit* nastavte na hodnotu, která je přijatelná pro hlasovou službu, tedy na hodnotu 400 kb/s. *Limit At* nastavte na 300 kb/s.

Bylo by možné také nakonfigurovat systém LLQ, ale konfigurace by byla stejná jako u systému CB WFQ a PQ. Správnou konfiguraci vámi vytvořených front si můžete ověřit podle směrovače R2, kde je konfigurace front kompletní.

A.2.3 Ověření nastavené konfigurace

Nastavení služeb

Na obou PC aktivujte *FilleZilla server start* a poté zapněte aplikaci *FilleZilla server*. V zobrazeném okně nastavte *Server Address: 127.0.0.1* a *Port: 14147*. Dále spusťte na obou PC také *FilleZilla* (klienta). Do položek programu *Fillezilla* na *PC1* napište následující údaje: *Hostitel: 172.27.141.10*, *Uživatelské jméno: user*, *Heslo: qosftppc2* a *Port: 21*. Na *PC2* nastavte stejné parametry, pouze hostitel je v tomto případě *PC1*, takže IP adresu nastavte na *172.27.141.2* a *Heslo: qosftppc1*.

Dále spusťte aplikaci *VLC* na *PC1* i *PC2*. Vytvořte stream otevřením nabídky *Média/Proud*. V nově otevřeném okně vyberte položku *Přidat*, kde vyberte video ze složky *D:\BP_DiffServ\VLC_stream*. Po přidání videa klikněte na *Proud* a dále na *Next*. V nabídce *Nový Cíl* vyberte *RTP/MPEG Transport Stream*. Nyní je nutné zadat IP adresu stanice, na které bude stream přijat. Klikněte tedy na *Přidat* a na *PC1* zadejte IP adresu *172.27.141.10* a na *PC2* IP adresu *172.27.141.2*. Port nechte nastavený na *5004*. Klikněte na *Next* a v dalším okně deaktivujte překódování. Vše potvrďte a v posledním okně klikněte na *stream*. Aby se streamované videa zobrazilo, spusťte znovu aplikaci *VLC*. Nyní vyberte nabídku *Média/Otevřít síťový proud*, kde na *PC1*, v záložce *Síť*, nastavte: *rtp://172.27.141.2:5004*. Stejný parametr nastavte také na *PC2*, ale IP adresu zvolte *172.27.141.10*. Stream by se měl, po kliknutí na *Přehrát*, zobrazit.

Zbývá nastavit hlasovou službu. Ve složce *D:\BP_DiffServ\VoIP* vyberte aplikaci *MicroSIP*. Aplikace se načítá delší dobu. Na *PC1* je možné se na *VoIP server* přihlásit přes účty *1001*, *1002*, *1003*, *1004*. Také na *PC2* byly vytvořeny čtyři účty *1017*, *1018*, *1019*, *1020*. Proto na *PC1* vyberte v nabídce *Menu* účet *1001* a vytočte číslo *1017*. **Na PC2 musí být aktivní účet 1017, aby mohl být hovor přijat.** Tento postup opakujte také pro účty *1002–1018*, *1003–1019* a *1004–1020*. Na obou PC vytočte ještě číslo *9999*, na kterém je spuštěna audio nahrávka.

Všechny služby jsou tedy spuštěny. Při neomezeném provozu dosahují přenosové rychlosti hodnot *90 Mb/s* pro přenos dat, *400 až 750 kb/s* pro streamované video a *320 kb/s* pro hlasovou službu. V dalších bodech budete omezovat šířku pásma, aby došlo k omezení nebo degradaci některých služeb.

Omezení šířky pásma na 3 Mb/s

Otevřete si záložku *Mangle*, v nabídce *IP/Firewall*, kde sledujte ve sloupci *Packets*, kolik paketů bylo označováno. Na druhé stanici pak ověřte, jestli všechny označované pakety jsou klasifikovány. V okně *Queue List* v záložce *Queue Tree* kontrolujte,

zdali všechny klasifikované pakety jsou zařazeny do dané fronty. V tomto okně pozorujte také přenosovou rychlost (*Avg. Rate*) všech služeb. Sledujte tuto možnost pro každou službu na obou stanicích.

V dalším postupu budete aktivovat vždy jeden systém front a sledovat jeho obsluhu. **Vždy před aktivováním daného systému front klikněte v záložce *Mangle* a *Queue Tree* na volbu *Reset All Counters*. Volbu v obou oknech a na obou stanicích se snažte aktivovat ve stejnou dobu.** Nyní výchozím nastavením všech front bude šířka pásma omezena na hodnotu 3 Mb/s. Aktivujte frontu typu FIFO. Pomocí FilleZilla přeneste z *PC1* na *PC2* soubor ze složky *D:\BP_DiffServ\FTP_Sdilena*. Podobně přeneste také soubor z *PC2* na *PC1*. Pokud se stream ukončil, spusťte ho znovu. Pozorujte kvalitu videa a posuďte kvalitu hlasu.

Dále aktivujte frontu PQ a FIFO zakažte. **Pokud byly soubory přeneseny, nebo došlo k ukončení streamu, opět služby spusťte.** Pozorujte, jakým způsobem služby zabírají šířku pásma a posuďte výhody a nevýhody prioritního systému front. Ověřte si také, zda počet klasifikovaných paketů pro jednotlivé služby odpovídá počtu paketů, které jsou zařazeny do front.

Stejným postupem povolte další systémy front, tak aby aktivní byl vždy pouze jeden systém. **Nezapomeňte vždy před aktivováním daného systému front zvolit volbu *Reset All Counters*.** Pozorujte kvalitu služeb v závislosti na použité frontě. Sledujte také, zda nedošlo k zahození paketů u některé služby. Uvědomte si u které služby může dojít k zahození paketů.

Omezení šířky pásma na 1,5 Mb/s

Všechny služby vypněte. Na RouterBoardu spusťte *New Terminal* a uveďte nastavení RouterBoardu do výchozího nastavení příkazem **system reset**. Poté se opět přihlaste ke směrovačům. Do okna *Files* zkopírujte soubory *R1/R2_1500kb.rsc*. Nahrané soubory importujte. Oba soubory obsahují kompletní konfiguraci. Zobrazte si nastavení front. Šířka pásma pro všechny fronty je omezena na 1,5 Mb/s. Prohlédněte si nastavení *Limit At* a *Max Limit* pro hlasovou službu a službu streamovaného videa. Opět spusťte všechny služby a aktivujte vždy jednu frontu. Pozorujte kvalitu služeb a počet zahozených paketů. Mělo by docházet k zahazování paketů u hlasové služby a služby streamovaného videa. Promyslete, jakým způsobem rozdělit šířku pásma, aby nedošlo k degradaci těchto služeb. Po skončení měření vypněte všechny služby a uveďte RouterBoard do výchozího nastavení

B OBSAH PŘILOŽENÉHO CD

Na přiloženém CD naleznete následující soubory:

- BP_xmarec13.pdf: elektronická verze této práce,
- složka Konfigurace_1500kb: obsahuje konfigurační soubory směrovače R1 a R2 pro laboratorní úlohu a šířku pásma 1500kb/s,
- složka Konfigurace_3000kb: obsahuje konfigurační soubory směrovače R1 a R2 pro laboratorní úlohu a šířku pásma 3000kb/s,
- složka Vysledna_konfigurace: obsahuje konfigurační soubory směrovače R1 a R2, kde je obsažena veškerá konfigurace potřebná pro správnou funkci laboratorní úlohy.